# Ergebnisbericht ZKI-Kommission Cloud

## Leitfaden zur Einführung von Cloud-Diensten an einer Hochschule

Zentren für Kommunikation und Informationsverarbeitung e.V.

# Inhaltsverzeichnis

# 1. Editorial – Ausgangslage und Motivation

Die Entwicklung von IT-Infrastrukturen in Richtung verschiedenartiger Cloud-Modelle ist eine unabweisbare Tatsache und impliziert weitreichende Konsequenzen für die Hochschul-IT auf allen Ebenen von Forschung, Lehre und Verwaltung. Neben den vielfältigen Chancen, die Versorgung eines Hochschulcampus zu verbessern, geht mit diesen Veränderungen eine Reihe von Herausforderungen einher, für deren Bewältigung Hochschulen Unterstützung benötigen. Die Verlagerung von Teilen der IT-Infrastruktur „off-campus“ hat entscheidende Auswirkungen auf die digitale Souveränität, die Gestaltung von Basisinfrastrukturen oder die Personalentwicklung, da neben neuen Möglichkeiten unerwartete Abhängigkeiten entstehen. Die Verfolgung von Cloud-Strategien kann zwar Grundlagen für eine höhere Resilienz bestimmter Dienste schaffen, muss jedoch dafür auf anderen Ebenen Vorkehrungen treffen. Neben der Betrachtung eines reinen (kurzfristigen) Nutzwerts geht es auch um eine gesellschaftliche Verantwortung und Vorbildfunktion.

Eine hohe Transparenz bei der Einführung von Cloud-Angeboten ist für alle Beteiligten sicherzustellen. Dafür bedarf es einer erweiterten Medienkompetenz sowohl bei den Forschenden als auch in den Verwaltungen als auch seitens der Studierenden und Mitarbeitenden. Die Implikationen von Datenschutz und Informationssicherheit bedürfen ebenso wie die Ausgestaltung der konkreten Anforderungen geeigneter Beratungsangebote und geschulten Personals. Hochschulleitungen sollten dabei auf eine Auswahl geprüfter Angebote aus dem kommerziellen und wissenschaftlichen Umfeld zurückgreifen können. Da viele Dienste in Zukunft von außerhalb des eigenen Campus bezogen werden, erfordert dies speziell qualifizierte Mitarbeitende und ausreichende Beratungskapazitäten, um Souveränität auch über zukünftige IT-Infrastrukturen zu gewährleisten. Die Entwicklungen implizieren ebenfalls eine Neuverteilung der Rollen zwischen der zentralen und dezentralen IT-Versorgung auf dem Campus. Während bereits jetzt kleinere Rechenzentren mit der anstehenden Breite von Aufgaben überfordert sind, gilt das umso stärker für die dezentralen IT-Abteilungen an einzelnen Fakultäten und Einrichtungen. Diese müssen ebenfalls in einer Cloud-Strategie berücksichtigt und geeignet eingebunden werden, da sie direkt mit den konkreten Bedarfen der einzelnen Disziplinen konfrontiert sind und die individuelle Nutzerunterstützung vor Ort leisten.

Cloud-Ansätze sind in einen strategischen Rahmen der Hochschule einzubetten. Ressourcen können sehr schnell ad hoc und damit sehr viel schneller als mit klassischen Methoden bereitgestellt werden. Zudem lassen sich Bedarfe von Projekten, Professuren, Campus-IT-Systemen deutlich besser hoch- und herunterskalieren. Diese können quasi sofort starten und sparen sich Auswahl, Ausschreibung, Organisation von Hosting/Anbindung, Setup und Hardware-Administration im laufenden Betrieb. Das hat direkte Auswirkung auf bestehende Abrechnungs- und Finanzierungsmodelle.

Die ZKI-Kommission Cloud wurde Ende 2019 gegründet und hatte ihre konstituierende Sitzung im Rahmen der ZKI-Frühjahrstagung 2020 in Leipzig. Die Kommission wird geleitet von Daniel Bündgens (Geschäftsführer, IT Center RWTH Aachen University) und Denise Dittrich (stellv. Abteilungsleiterin Systeme und Betrieb, IT Center RWTH Aachen University). Ziel der Arbeitsgruppe war die Erstellung eines Leitfadens, der die Einführung und Nutzung von Cloud-Produkten beschreibt. Der nun vorliegende Leitfaden soll für alle ZKI-Mitgliedshochschulen als Best Practice dienen und enthält sowohl allgemeine Richtlinien als auch konkrete produktbezogene Empfehlungen.

## 1.1. Aufbau des Dokuments

Die Kommission hat für die Ausarbeitung des Leitfadens verschiedene Arbeitsgruppen gebildet, die sich wiederum speziellen Themen gewidmet haben:

- Cloud-Strategie
- organisatorische Einführung
- technische Anbindung
- Datenschutz und Datensicherheit
- Vertragliches

Das Gesamtergebnis aller Arbeitsgruppen spiegelt sich in diesem Dokument wider.

Das Dokument ist so gegliedert, dass es der Reihenfolge der organisatorisch notwendigen Schritte zur Einführung eines Cloud-Produkts entspricht. Dabei wird davon ausgegangen, dass es sich um die Einführung eines ersten (größeren) Cloud-Angebots handelt und somit zunächst generelle Fragestellungen behandelt werden müssen. Bei der Einführung weiterer Cloud-Angebote kann dann ähnlich verfahren werden, allerdings einzelne Schritte ausgelassen oder verkürzt werden.

Die einzelnen Kapitel dieses Dokuments sind wie folgt strukturiert: Jedes Kapitel beginnt mit einem Executive Summary des jeweiligen Inhalts. Die Zielgruppen sind entweder direkt am Anfang des Kapitels oder, sollte es sich unterscheiden, am Anfang des Unterkapitels genannt.

Anschließend werden die Handlungsfelder und Unterthemen genauer beschrieben und letztendlich Empfehlungen ausgesprochen werden. Hierbei werden die einzelnen Adressaten separat angesprochen. Je nach Thema zählen hierzu z.B. Hochschulleitungen, RZ-Leitungen oder Fakultäten/Institute (fachspezifischer).

Im Anhang (Kapitel 5) werden anbieterspezifische Beispiele für konkrete Verträge und Umsetzung aufgezeigt sowie die Autoren des Dokuments und Mitglieder der Kommission genannt.

## 1.2. Weitere Ergebnisse der Kommission

Neben diesem Leitfaden ist im Rahmen der Kommissionsarbeit auch ein weiteres Dokument entstanden, dass sich mit der politischen Dimension der Cloud-Angebote und den Auswirkungen auf die Hochschularbeit befasst, da Clouds einen weiteren Paradigmenwechsel in der IT-Versorgung darstellen. Sie benötigen für ihre sichere und nachhaltige Nutzung einen geeigneten organisatorischen und rechtlichen Rahmen.

Die laufenden Überlegungen bekommen daher eine politische Dimension, die sich neben rechtlichen und regulatorischen Rahmensetzungen mit Marktimperfektionen und gesellschaftlichen Gestaltungsspielräumen auseinandersetzen sollte. So genügen die klassischen Verhandlungsstrategien in der Vorbereitung von großen Software- und Cloud-Verträgen – selbst auf Leitungsebene einer Hochschule – nicht mehr, um diese Entwicklungen im eigenen Sinne zu kontrollieren und positiv mitzugestalten. Strategien im Umgang mit Cloud-Angeboten sollten daher um einen globaleren Ansatz komplementiert werden, um dem strukturellen Charakter von Software vergleichbar mit einer Grundversorgung (Energie, Wasser) deutlich stärker Rechnung zu tragen.

Diese Diskussionen wurden im Rahmen der ZKI-Kommission Cloud begonnen und zusammengestellt. Gestaltende Elemente könnten von potenziell sehr langlaufenden Vereinbarungen mit Anbietern

über Alternativen wie Genossenschaftsmodelle bis hin zur klaren Regulierung und Neugestaltung des Marktes reichen. Verhandlungen sollten politische Dimensionen umfassen, wie bspw. eine Vertrauensbildung durch die Offenlegung von Preisbildung und Source Code. Klare Umstiegsoptionen mit der Übernahme von Konversionskosten könnten ebenso ins Auge gefasst werden wie eine Reform des Patent- und Urheberrechts bei Software, die in der jetzigen Form eher den Markt einseitig manipulieren, als Innovation befördern. In allen Fällen sind Gesetzgeber und Exekutive ebenfalls gefragt.

# 2. Strategische Entscheidung

*Zielgruppe: Entscheidungsträger in der Hochschule, z.B. RZ-Leitung, Hochschulleitung*

*Der Paradigmenwechsel in der IT-Versorgung zu Cloud-basierten Angeboten ist unausweichlich, deshalb sollten die Hochschulen eine Cloud-Strategie für ihre Campus-IT gemeinsam mit den lokalen Akteuren (Nutzern) erarbeiten und diese übergreifend abstimmen. Diese sollte Aspekte wie Multi-Vendor- und Exit-Strategien zur Wahrung der Handlungsfähigkeit bzw. digitalen Souveränität enthalten, aber auch Rahmenbedingungen wie eine Digitalisierungsstrategie sowie die veränderte Verteilung von Verantwortlichkeiten in der IT berücksichtigen.*

Ein wesentlicher Schritt auf dem Weg zur Nutzung von Cloud-Angeboten sind grundsätzliche, strategische Planungen und Entscheidungen zur Ausrichtung der eigenen Hochschule. Welche Anforderungen ergeben sich aus der Hochschul- bzw. IT-Strategie? Und was kann dabei helfen, diese zielgerichtet, wirtschaftlich und skalierbar umzusetzen? Hier kann die Cloud ein wesentlicher Baustein sein. Dabei ist es wichtig, eine Cloud-Strategie – als Teil der IT-Strategie – für die eigene Hochschule zu entwickeln. Diese bestimmt maßgeblich die Rahmenbedingungen, unter denen Cloud-Angebote nutzbar gemacht werden können.

Neben der strategischen Entscheidung durch die Hochschulleitung und das CIO/CDO-Gremium müssen weitere Gremien wie z.B. Rektorate, Personalvertretungen, Gleichstellungs- und Schwerbehindertenbeauftragte eng mit eingebunden werden. Die stärkere Nutzung von Cloud-Angeboten führt perspektivisch auch zu Veränderungen in Bezug auf das lokale eingesetzte Personal. So werden bestimmte Tätigkeiten wie z.B. Hardware-Aufbau und Wartung zunehmend weniger. Die IT-Fachkräfte müssen stärker prozessual denken und auch wesentlich intensiver mit den Fachbereichen, Instituten und Fachabteilungen interagieren. Damit sind Skills wie Prozessdenken, Kommunikation, Agilität etc. immer stärker gefragt. Das muss durch entsprechenden Schulungsaufwand, aber auch im Rahmen von Neu- und Nachbesetzungen berücksichtigt werden. Gerade hierdurch können sich Widerstände ergeben, die es frühzeitig auszuräumen gilt.

Ein weiterer, nicht zu unterschätzender Aspekt ist die klare Zuordnung von Verantwortlichkeiten. Diese sollten als Rahmenparameter in der Cloud-Strategie definiert werden und dienen ebenfalls als Grundlage für jede Beschaffung von Cloud-Angeboten.

Die Entwicklung von IT-Infrastrukturen in Richtung verschiedenartiger Cloud-Modelle ist eine unabweisbare Tatsache und impliziert weitreichende Konsequenzen für die Hochschul-IT auf allen Ebenen von Forschung, Lehre und Verwaltung. Neben den vielfältigen Chancen, die Versorgung eines Hochschulcampus zu verbessern, geht mit diesen Veränderungen eine Reihe von Herausforderungen einher, für deren Bewältigung Hochschulen Unterstützung benötigen. Die Verlagerung von Teilen der IT-Infrastruktur „off-campus“ hat entscheidende Auswirkungen auf die digitale Souveränität, die Gestaltung von Basisinfrastrukturen oder die Personalentwicklung, da neben neuen Möglichkeiten unerwartete Abhängigkeiten entstehen. Die Verfolgung von Cloud-Strategien kann zwar Grundlagen für eine höhere Resilienz bestimmter Dienste schaffen, muss jedoch dafür auf anderen Ebenen Vorkehrungen treffen. Neben der Betrachtung eines reinen (kurzfristigen) Nutzwerts geht es ebenfalls um eine gesellschaftliche Verantwortung und Vorbildfunktion.

## 2.1. Digitale Souveränität

Die meisten kommerziellen Angebote verfolgen ein klares Plattformmodell, das ein sehr breites Angebot an Diensten bei gleichzeitig hoher Integration anstrebt. Der Nutzwert ist in der Phase des derzeit stattfindenden Paradigmenwechsels für die Kundenseite sehr attraktiv, da viele Anbieter noch in der Kundenbindungsphase sind und versuchen, sich durch aggressives Pricing einen signifikanten Marktanteil zu sichern. Mit der sich andeutenden hohen Konzentration des Marktes auf wenige Anbieter werden Monopolisierungstendenzen mit ihren typischen Kostenimplikationen deutlich zunehmen. Eine (scheinbare) Alternativlosigkeit zu diesen Angeboten verschlechtert die eigene Verhandlungsposition deutlich. Zukünftige Verträge laufen in die Gefahr, vergleichbare Leistung für deutlich höhere Aufwendungen einkaufen zu müssen, die dann aus anderen Teilen des eigenen Haushalts „herausgeschwitzt“ werden, was die eigene Lage zusätzlich verschlechtert und den Bewegungsspielraum einschränkt.

Digitale Souveränität kann durch verschiedene Ansätze sichergestellt werden:

- eine angepassten Exit-Strategie für wichtige Services in der Cloud
- eine Dual/Multi-Vendor-Strategie
- das Vorhalten von wichtigen/entsprechenden Services „on Premise“
- langfristige strategische Planungen und Abstimmung auf höheren Ebenen

Der Weg in die Cloud schafft die Möglichkeit, neue vielfältige Dienste anzubieten, impliziert jedoch neuartige Risiken, die in der Betrachtung und Entwicklung einer Strategie berücksichtigt werden müssen. Hierzu zählen auch die Auswirkungen auf die Resilienz der Einrichtung: So sind viele Angebote bereits inhärent auf eine höhere Ausfallsicherheit und Skalierbarkeit angelegt, hängen dafür vermehrt von den Basisinfrastrukturen, wie Netzwerk, Identity und Access Management ab. Entscheiderinnen und Entscheider sollten ihre gesellschaftliche Verantwortung wahrnehmen und darauf achten, dass keine heutigen und zukünftigen Mitglieder der Einrichtung von wichtigen Angeboten ausgeschlossen werden. Dies stellt vermehrt Anforderungen an eine ausreichende Medienkompetenz und an die Ausrichtung der Personalentwicklung. Die Stärkung der individuellen digitalen Kompetenzen (Data Literacy) ist eine der Voraussetzungen für unabhängiges Handeln, orientiert an europäischen Werten wie Datenschutz, Vertrauen, Transparenz, freier Marktzugang sowie Souveränität und Selbstbestimmtheit.

## 2.2. Dual-/Multi-Vendor- oder Exit-Strategie

Um die Abhängigkeit von einzelnen Cloud-Anbietern zu verringern sowie Vendor Lock-ins zu vermeiden und auf diese Weise die (digitale) Souveränität der Hochschule zu stärken, sollte eine Dual- oder Multi-Vendor-Strategie in Betracht gezogen werden. Diese erlaubt, auf Änderungen bei rechtlichen Rahmenbedingungen (vgl. Urteil zum Privacy Shield[1]) zu reagieren. Eine abgewandelte Option besteht in einer Exit-Strategie, die versucht, sowohl den personellen als auch den finanziellen Aufwand eines Ausstiegs abzuschätzen. Gerade der Schritt zurück zu Installationen an der eigenen Hochschule erfordert das Aufrechterhalten eigener Ressourcen oder zumindest die Fähigkeit, diese kurzfristig

[1] https://www.gdd.de/eu-us-privacy-shield-schrems-ii-urteil/handlungsempfehlungen-eugh-eu-us-privacy-shield-und-eu-standardvertragsklauseln

(wieder) aufzubauen. Dieses Aufrechterhalten eigener Ressourcen widerspricht aber einer der Erwartungen an den Schritt in die Cloud, nämlich der erhofften Kosteneinsparung bei gleichzeitigem Gewinn an Skalierbarkeit.

Dabei gilt es, Folgendes zu berücksichtigen:

- Bedarfe (er-)kennen: Da Angebote im Cloud-Bereich sehr vielfältig sind, müssen die Bedarfe der Hochschule oder einzelner Nutzer bekannt sein. Die angebotenen Cloud-Dienste sollten darauf abgestimmt sein.

- Geeignete Anbieter finden: Zu berücksichtigen sind neben dem Angebot zudem Rahmenbedingungen wie bspw. Serverstandort, Herkunftsland des Anbieters, Referenzen o.Ä.

- Balance zwischen Souveränität und Aufwand: Nicht für alle Cloud-Produkte erscheint es sinnvoll (oder realistisch), mehrere Anbieter mit dem benötigten Angebot zu finden. An dieser Stelle ist es wichtig, den Aufwand für die Einführung/Nutzung mehrerer Anbieter dem tatsächlichen Nutzen gegenüberzustellen. Berücksichtigt werden sollte immer, wie groß der Schaden sein kann, den die Hochschule durch die Abhängigkeit von einem Anbieter in einem speziellen Fall davontragen kann (= Risikobewertung). Eine Abstimmung unter Hochschulen oder sogar eine Kooperation auf Landesebene kann hier eine Möglichkeit sein, die Balance herzustellen.

- Berücksichtigung von Exit oder Wechsel-Strategien bei einer Cloud-Ausschreibung

### 2.2.1. Exit-Strategie

Am einfachsten gestaltet sich ein Ausstieg bei der Nutzung von „Infrastructure as a Service“ (IaaS). Dies beinhaltet Rechenleistung, einfachen Datenspeicher und Netze. Bei „Platform as a Service“ (PaaS) wird es bereits komplizierter. Hier wird eine komplette Plattform mit unterschiedlichen Diensten und bestehenden Prozessen genutzt. Es ist schwieriger, diese aufzulösen, da insbesondere die Prozesse und unterstützenden Dienste im eigenen Rechenzentrum abgebildet werden müssen. Die Daten können meist nur unter größerem Aufwand extrahiert werden (vgl. Ausführung in 2.2.3). Bei „Software as a Service“ (SaaS) ist teilweise keine Übernahme der Daten vorgesehen oder mit extra Kosten verbunden. Gegebenenfalls können Zusicherungen des Anbieters zum standardisierten Datenexport im Zuge einer Ausschreibung bzw. im Zusammenhang mit der Beschaffung eingeholt werden.

| Modell | Exit |
|---|---|
| **IaaS** | Möglich, sofern entsprechende Infrastruktur „on premise“ vorhanden ist. |
| **SaaS** | Schwierig, da meist ein Export aller Daten und ihrer Kontexte (inkl. Berechtigungen, Metadaten etc.) gar nicht möglich ist. Auch wenn es gelingt, Daten aus der Cloud lokal zu sichern, lassen sich die eigentlichen in der Cloud genutzten Funktionalitäten und Interaktionen verschiedener Komponenten meist nicht lokal replizieren. Sollte es sich hier um geschäftskritische Prozesse handeln, z.B. Interaktionen im Lehr- und Studienbetrieb oder in Forschungsprojekten, muss das resultierende Risiko genau abgewogen werden. Alternative On-Premise-Lösungen müssten aufgebaut werden. |
| **PaaS** | Hier müssen je nach PaaS nicht nur die zugrunde liegende Hardware und die verwendeten/generierten Daten bei einem Exit-Szenario betrachtet werden, sondern auch Prozesse (z.B. CICD) oder auch schon vorhandene Software-Komponenten/Algorithmen (z.B. KI-Module) |

Wichtig ist, dass Cloud-Anwendungen so generisch wie möglich unter Einsatz von offenen Schnittstellen und Protokollen konzipiert werden. Die Interoperabilität kann mit standardisierten oder offengelegten Schnittstellen sichergestellt werden. Der Einsatz von anbieterspezifischen Cloud-Diensten (Vendor Lock-in durch anbieterspezifische Support-Funktionen) sollte auf ein Minimum reduziert werden. Die Funktionalität, eigene oder Services/Anwendungen von anderen Anbietern einzubinden, sollte gegeben sein.

Ein weiterer wichtiger Punkt besteht in der Portabilität von Daten und Anwendungen. Es sollten vorzugsweise standardisierte Technologien wie Container verwendet werden. Auch „Infrastructure as Code“ erlaubt schneller, die Infrastruktur hochzuziehen und damit schneller zwischen Anbietern zu wechseln. Industriestandards zur Senkung von Interoperabilitäts- und Portabilitätsproblemen sind ebenfalls zu nutzen.

Vor dem Start sollten unbedingt die vertraglichen Bedingungen einer Exit-Möglichkeit (Portabilität der Daten in einem festgelegten Format) bspw. als Punkt in den Ausschreibungen geprüft und die damit einhergehenden Kosten offengelegt werden. Oft fallen für den Datenexport zusätzliche Kosten an. Die Bedingungen zur Beendigung des Vertrags müssen deshalb vorab festgelegt werden.

### 2.2.2. Dual/Multi Vendor Management

Da reine Exit-Strategien nur begrenzt anwendbar sind, empfiehlt es sich, mindestens eine Dual- oder aber besser eine Multi-Vendor-Strategie zu verfolgen. Durch die Verteilung der Workloads auf mehrere Anbieter wird zum einen die Abhängigkeit einer Hochschule von einem Anbieter verringert, zum anderen der Druck auf einzelne Anbieter erhöht, wettbewerbsfähig und kundenorientiert zu bleiben.

Mögliche Multi-Vendor-Strategien könnten beinhalten:

- mehrere große Cloud-Anbieter der Hochschule verfügbar machen, die ein ähnliches Portfolio haben (z.B. Microsoft Azure und Amazon AWS für IaaS-Angebote)
- einen großen Cloud-Anbieter mit mehreren kleinen Anbietern zu kombinieren, die jeweils einen Teil des Angebots abdecken (z.B. Microsoft M365 + Zoom + Open Telekom Cloud für IaaS in Deutschland)
- eigenes IaaS-Angebot für wissenschaftliches Computing (mit eventuell Spezialkomponenten wie GPUs) und allgemeine Bedarfe der Forschung vorhalten

Bei der Auswahl geeigneter Cloud-Anbieter steht den Hochschulen z.B. über den OCRE-Rahmenvertrag (vom GÉANT/DFN verhandelte Angebote; siehe Kapitel 5.23) eine Vielzahl an Anbietern zur Verfügung. Die Auswahl der „richtigen“ Anbieter ist dabei individuell von jeder Hochschule zu treffen, dabei können u.a. folgende Kriterien berücksichtigt werden:

- Bedarfe in der Hochschule
- Kosten: Vergleich eines konkreten Nutzungsszenarios bei diversen Anbietern
- Lokation des Cloud-Anbieters (nicht der Rechenzentren!): amerikanisch vs. europäisch vs. deutsch
- Klassifizierung der Daten, die in der Cloud abgelegt werden (vgl. Ausführungen in Kapitel 3.21) und wodurch ggf. rechtliche Rahmenbedingungen erwachsen, die einzuhalten sind (z.B. Datenhaltung in Deutschland)

- vorhandene Features, gerade im PaaS-Bereich: hier unterscheiden sich die reinen Infrastrukturanbieter von z.B. AWS oder Azure

- angebotene zusätzliche Leistungen, z.B. Support, Workshops, …

Sofern verschiedene Cloud-Anbieter an einer Hochschule zum Einsatz kommen, muss es für die Nutzenden Leitlinien und Beratung geben, die bei der Auswahl aus den an der Hochschule vorhandenen Anbietern unterstützen. Die Unterstützung sollte zentral durch die Hochschule (z.B. durch das Rechenzentrum) angeboten werden.

### 2.2.3. Datensicherung/Backup

Datensicherung, Backup und Archivierung sollten als Teil einer Exit- und Multi-Vendor-Strategie mitbetrachtet werden. Neben den vom Cloud-Anbieter vorgenommenen Maßnahmen sind Konzepte zur Sicherung der Daten in der Cloud notwendig, um hier die Datenhoheit zu behalten. Grundsätzlich gibt es mehrere Varianten:

1. Daten werden zusätzlich (als Zweitkopie) in der Cloud gesichert (z.B. geo-redundant).
2. Daten werden zusätzlich „on Premise“ gesichert. Hier ist zu beachten, dass je nach Cloud-Anbieter und vorhandenem Vertrag der ausgehende Datenverkehr Cloud ⇒ „on Premise“ ggf. erhebliche Transfers verursachen kann und potenziell zu einem Kostentreiber wird.

Darüber hinaus sollte beachtet werden, dass für die unterschiedlichen Servicemodelle (XaaS) unterschiedliche Konzepte zur Datensicherung benötigt werden. Es ist zu prüfen, inwieweit hier nur eine zusätzliche Speicherung der Daten zur Sicherung der Datenhoheit erfolgt oder ob darüber hinaus der Fall von Datenverlust abgedeckt werden soll, der auch eine entsprechende Wiederherstellung der Daten bedingt.

Weiterhin sollte berücksichtigt werden, dass insbesondere bei spezielleren, proprietären Formaten eine enge Beziehung zwischen Daten und Applikationen besteht. Hier sollte durch eine geeignete Formatwahl (so überhaupt möglich) sichergestellt werden, dass Daten auch außerhalb des jeweiligen Angebots nutzbar bleiben.

## 2.3. Strategischer Rahmen

Im Rahmen der Digitalisierungsstrategie der jeweiligen Hochschule sollte dargelegt werden, welche Chancen und Risiken in der digitalen Transformation mit Fokus auf eine Cloud-Strategie liegen, wie die Chancen genutzt werden können und wie mit etwaigen Risiken verantwortungsvoll umgegangen werden kann. Im Einvernehmen mit den strategischen Leitlinien der Hochschule sind die inhaltlichen und strategischen Fragen der Digitalisierung in den Kernaufgaben Lehre, Forschung und Administration auszuführen. Die Darlegung der Maßnahmen und ihre Umsetzung ist zu beschreiben und regelmäßig zu evaluieren und zu aktualisieren. Die Cloud-Strategie muss daher ein Teil der Digitalisierungsstrategie sein.

Berufungsverhandlungen sind wesentliche Schlüsselmomente für die Entwicklung zukünftiger Professuren sowie der beheimatenden Fakultät und ihrer Forschungsinfrastrukturen. Die Steuerung der Mittelflüsse erlaubt strategische Einflussnahmen auf die Entwicklungen an der eigenen Hochschule. Das impliziert die Definition klarer Prozesse zwischen der Hochschulleitung, den an der Berufung beteiligten Fakultäten und den Berufenen.

Für neue Professuren können sich deutliche Startvorteile ergeben, da nicht erst aufwendig eigene Infrastrukturen aufgebaut werden müssen, um mit der eigenen Forschung zu beginnen. Insbesondere am Anfang fallen viele Aufgaben parallel an, sodass Entlastungen im Bereich der IT-Versorgung sich positiv auf die Produktivität der neuen Hochschulmitglieder und damit der Gesamteinrichtung auswirken sollten.

### 2.3.1. Governance und Kommunikation

Governance soll Mitsprache und Mitentscheidung, mithin Transparenz und Partizipation auf den verschiedenen Ebenen sicherstellen. Sie definiert zudem den Ordnungs- und Handlungsrahmen – regelt Rollen, Funktionen und Aufgaben als eine Basis der Digitalisierungsstrategie der Hochschule. Das Zusammenwirken von zentralen und dezentralen Einheiten und die Einbeziehung der Nutzerseite aus Lehre, Forschung und Administration sowie die zugehörigen Koordinierungs-, Aufsichts- und Steuerungsstrukturen sollten in einem IT- bzw. Digitalisierungs-Governance-Framework beschrieben sein. Die systematische Erweiterung der IT- bzw. Digitalisierungs-Governance für die Einbindung von Cloud-Lösungen sollte frühzeitig erfolgen.

Umfang und Verfügbarkeit von IT-Diensten sind zentrale Punkte, die zwischen den verschiedenen Beteiligten an der Hochschule beständig ausgehandelt werden müssen. Hierzu zählen eine sinnvollerweise institutionalisierte Form des User-Feedbacks sowie geeignete Gremien, die regelmäßig die Strategien weiterentwickeln und generelle Entwicklungen im Blick behalten sowie beratend wirken können. Governance arbeitet als Schnittstelle zwischen strategischen Vorgaben und ihrer operativen Umsetzung. Zu den Fragen, die in diesem Zusammenhang zu klären sind, zählen: Welche Dienste und Daten sollten in die Cloud? Was muss in die Cloud? Was darf nicht in die Cloud? Solche Fragen sind einer systematischen Betrachtung im Rahmen des Prozessmanagements zu unterziehen.

Mit der Nutzung verschiedener externer Angebote verringern sich die Optionen zur direkten Einflussnahme und unterstehen nicht mehr der eigenen Governance. In dem Moment, wo bestimmte Funktionen und Gestaltungsoptionen zu einem Cloud-Anbieter verschoben werden (seien es Aspekte von Green-IT, Datenschutz, Nachhaltigkeit oder die Ausgestaltung von Features), sollte die Hoheit über diese „mitwandern“ und diese Entscheidungen, die man „on Premise“ treffen würde, nicht komplett aus der Hand gegeben werden. An dieser Stelle muss überlegt werden, wie die gewünschte Einflussnahme auf rechtliche Rahmensetzungen[2], Umfang und Ausgestaltung von Features der verschiedenen Angebote erfolgen soll. So möchte man eventuell über die Ausgestaltung einer nachhaltigen Energieversorgung ebenso mitbestimmen wie einzelne Funktionen der Software als unerwünscht abwählen, wie etwa das Profiling oder die Verhaltenskontrolle der Arbeitnehmerinnen und Arbeitnehmer. Eine Einflussnahme wird sich in vielen Fällen auf die Gestaltung von Auftragsdatenverarbeitungsverträgen oder Ausschreibungen verlagern.

Kommunikation und Öffentlichkeitsarbeit sollten komplementär zur Governance mitbedacht werden. Sie können sich dabei etablierter Kanäle seitens der Rechenzentren, der zentralen Verwaltungen sowie der Fakultäten und Institute bedienen.

[2] S. hierzu das von der ZKI Kommission Cloud erstelle Dokumente zur politischen Dimension der Cloudnutzung.

### 2.3.2. Nachhaltigkeit

Das Thema Nachhaltigkeit rückt ebenso wie die Digitalisierung in den Fokus der Hochschulstrategie und gewinnt zunehmend an Wichtigkeit. Insbesondere durch die Pandemiesituation 2020/2021 ist weltweit das Bewusstsein für Nachhaltigkeit massiv gestiegen. Dabei gibt es mindestens zwei zu bewertende Punkte: zum einen die Energieversorgung der Rechenzentren, zum anderen die Nutzung von IT-Ressourcen. Insbesondere Hardware zeichnet sich durch immer kürzere Lebenszyklen aus, die durch eine rasante technische Entwicklung erzeugt werden. Da gerade bei öffentlichen Einrichtungen auf dieses Thema geschaut wird und durch Landespolitik und Bundesregierung entsprechende $CO_2$-Ziele formuliert werden, können Cloud-Strategien zu einer nachhaltigen und klimaneutralen Ausrichtung beitragen.

## 2.4. Rekalibrierung der Aufgabenverteilung der Campus-IT

Für eine Hochschule sind je nach Anforderung eine Reihe von Abwägungen zwischen verschiedenen Cloud-Ressourcen – kommerziell vs. eigene Ressourcen bzw. zentrales vs. dezentrales Cloud Management – zu treffen. Eine zentrale Steuerung und Abstimmung erlaubt die Umsetzung der Ziele Multi-Vendor- und Exit-Strategie, bspw. durch eine übergreifende Abstimmung/Kooperation mit anderen Hochschulen, durch die Verteilung der Anfragen auf verschiedene Anbieter. Die Umsetzung von Cloud-Strategien impliziert zudem eine Verschiebung von personellen und Hardware-Ressourcen und geht dabei mit einer gewissen Konsolidierung und Zentralisierung dieser Ressourcen einher. Dies kann bisher stark verteilte Aufwände für die physische und die Netzwerkabsicherung sowie für Klima-, Energie- und Netzwerkinfrastrukturen zusammenfassen und dabei die Qualität des Angebots erhöhen oder Kosten einsparen. Das erlaubt eine stärkere Spezialisierung des Betriebspersonals auf mehreren Ebenen. Bei lokalen Angeboten umfasst das den Campus der eigenen Hochschule, bei vielen kommerziellen Angeboten bleiben am Ende nur noch die Endbenutzergeräte vor Ort. Im Fall des Angebots eigener Ressourcen oder sogar für weitere Hochschulen verbreitern sich die Basisaufgaben, wie die Bereitstellung von Serverräumen, die Netzwerkanbindung, die Beschaffung/Erneuerung von Hardware, und viele Aspekte der Basisadministration (Hardware und Cloud-Infrastruktur) können zentralisiert werden. Alle inhaltlichen Aufgaben im Rahmen von Forschung, Lehre und Verwaltung sollten auf Basis dieser Grundinfrastrukturen oder kommerziellen Angebote weiterhin vor Ort geleistet werden. Cloud-Ansätze spielen besonders klar auf höheren Dienstschichten, wie Fachanwendungen und -diensten, ihre Vorteile aus. Zunehmend setzt sich daher in Projekten und Professuren die Erkenntnis durch, dass den meisten Forschenden eher mit einer inhaltlichen Unterstützung gedient ist, als wenn das IT-Personal mit dem Nachbau von Basisinfrastrukturen für Storage und Computing beschäftigt wird.

Die notwendigen Beratungs- und Support-Strukturen erfordern neben technischem Cloud-Know-how entsprechend ausgestattete Rechtsabteilungen und Datenschutz- und Informationssicherheitsbeauftragte. In vielen Fällen ist vor der Umsetzung einer Cloud-Strategie eine rechtliche Beratung sinnvoll, die für die Anwenderseite auf die geplanten Nutzungsszenarien fokussiert und Hochschul- und RZ-Leitungen zur Abschätzung der Implikationen der verschiedenen Angebote verhilft. Ebenso sollten Personalressourcen für die regelmäßige Aktualisierung entsprechender Empfehlungskonzepte mit Maßnahmen und Zielen eingeplant sein.

Im Bereich des Supports muss ein an die Hochschule angepasstes Konzept entwickelt werden, welche Cloud-Anbieter bis zu welchem Grad unterstützt werden. Dazu zählen sowohl das Zusammenspiel der verschiedenen Support-Level (1st, 2nd etc.) innerhalb der Hochschule als auch eine entsprechende Berücksichtigung des Supports seitens des Cloud-Anbieters. Zentrale Strukturen helfen, Bedarfe zu erkennen und Know-how zu bündeln. Bei weniger ausgeprägter Nutzung (z.B. bzgl. eines

konkreten Cloud-Anbieters) in der Hochschule bietet sich hier aber auch an, mehrere Hochschuleinrichtungen zu verbinden und z.B. dezentrale und zentrale Strukturen für Beratung und Support zu vereinen.

## 2.5. Anforderungen an die Cloud-Strategie, Datenhoheit und Verantwortlichkeiten

### 2.5.1. Anforderungen an Hochschulen zur Erstellung einer Cloud-Strategie

- Es sind alle Entscheidungsträgerinnen und Entscheidungsträger angemessen vor dem Beginn der Dienstnutzung zu involvieren, insbesondere IT-Leitungsverantwortliche, Datenschutzbeauftragte, Informationssicherheitsbeauftragte, der Personal- bzw. Betriebsrat und die Anfordernden.

- Es sind die rechtlichen Anforderungen betreffend Datenschutz und Informationssicherheit zu klären sowie regelmäßig Fragen mit Blick auf Auftragsverarbeitung, Geheimhaltungspflichten (z.B. durch Geheimhaltungsvereinbarungen in Drittmittelprojekten) und Geheimnisschutz zu beachten.

- Es ist unabdingbar, dass Hochschulen vor der Auslagerung von Informationen eine klare Stellungnahme zur internen Informationsklassifizierung und davon abgeleitet Schutzmaßnahmen festlegen[3]. Darauf aufbauend ist festzulegen, welche Informationen in der Cloud verarbeitet werden dürfen und welche nicht.

- Die Leitungsebene ist und bleibt für die Steuerung der Risikobehandlung verantwortlich und kann im Rahmen der gesetzlichen Vorgaben ungenügend behandelte Risiken akzeptieren (Risikoübernahme).

- Es ist eine regelmäßige Evaluation und Überprüfung von Dienstleistern sowie der internen und externen Schutzmaßnahmen (beim Dienstleister) vorzusehen.[4]

### 2.5.2. Datenhoheit

Eines der Hauptrisiken beim Einsatz von Cloud-Anbietern ist der Verlust der Datenhoheit der Hochschule. Datenhoheit liegt für Hochschulen als Träger der Datenhoheit vor, wenn

- die Daten jederzeit verfügbar sind,

- die Institution bezüglich der Daten verfügungsbefugt ist,

- die Daten im jeweils genutzten Cloud-System vertraulich behandelt werden und

---

[3] Beispiel: Musterrichtlinie zur Klassifizierung von Informationen der bayerischen Hochschulen und Universitäten und das dazugehörige Informationsschutzkonzept:
https://www.hs-augsburg.de/Rechenzentrum/Stabsstelle-Informationssicherheit.html

[4] Siehe BSI IT-Grundschutz-Kompendium, OPS.2.1 Outsourcing für Kunden, inkl. Umsetzungshinweise

- das genutzte Cloud-System integer ist.

Datenhoheit ist kein eigenständiges Recht, sondern ein Sammelbegriff, der die Schutzziele der Informationssicherheit – Verfügbarkeit, Vertraulichkeit und Integrität – adressiert und das rechtliche Element der Verfügungsbefugnis enthält. Die angeführten Aspekte müssen bei der Ausgestaltung von Verträgen mit dem Cloud-Anbieter unbedingt beachtet und im Benehmen mit diesem die technisch-organisatorischen Maßnahmen im Rahmen eines Informationssicherheitskonzepts zur Sicherstellung der Datenhoheit der Institution definiert, vertraglich fixiert und kontinuierlich geprüft werden.

### 2.5.3. Verantwortlichkeiten

Beim Einsatz von Cloud-Lösungen teilen sich alle Beteiligten die Verantwortlichkeiten für die Sicherheit der Verarbeitung:

- der Cloud-Anbieter (Cloud Service Provider – CSP)
- der Cloud-Kunde (die Hochschule)
- der Endnutzer (Beschäftigte bzw. Studierende)

Der Cloud-Anbieter ist verantwortlich für alle Angelegenheiten des Schutzes vor physischen Schäden, der Hosting-Infrastruktur und des Netzwerks. Unter anderem sehen ISO 27001 und SOC 2 für den physischen Aspekt z.B. den Schutz von Servern, der Verkabelung oder des Datenspeichers vor schädlichen Außenwirkungen und gefährlichen Eingriffen vor.

Die Institution und der Cloud-Anbieter teilen sich je nach eingesetzter Lösung die Verantwortung für das sichere Funktionieren und den Schutz der eingesetzten Applikationen vor potenziellen Gefährdungen. Die Institution trägt die Verantwortung für das Identity und Access Management, also für die Identifizierung der Mitarbeitenden und deren entsprechender Nutzungsbefugnisse im Rahmen des eingesetzten Systems. Der Schutz der Endgeräte, über die sich die Mitarbeitenden in der Institution oder mobil mit dem Cloud-Dienst verbinden, liegt gleichermaßen in der Verantwortung des Cloud-Kunden und muss durch diesen sichergestellt werden.

Die Endnutzer tragen die Verantwortung für die Cloud-Daten, die erfahrungsgemäß nicht immer in der Cloud bleiben und auf mobilen Endgeräten (Smartphones, Notebooks, Tablets) verarbeitet und gespeichert werden. Die Hochschule muss hier besonderen Wert auf die Schulung und Sensibilisierung der Mitarbeitenden im Umgang mit Cloud-Diensten und der damit in Zusammenhang stehenden Datennutzung legen, gerade auch mit Blick auf die Informationsklassifizierung und die Risiken der Cloud-Nutzung.

Je nach eingesetztem Cloud-Dienst (Iaas, PaaS, SaaS etc.) variiert der Grad der Verantwortlichkeit zwischen den einzelnen Akteuren. Ziel muss ein hohes Sicherheitsniveau bei der Verarbeitung von Daten beim Cloud-Anbieter und bei der Institution mit deren Mitarbeitenden sein.

## 2.6. Empfehlungen

### 2.6.1. Empfehlungen für Hochschulleitungen

- Festlegung der Hochschulstrategie: Abwägung zwischen zentralem (andere Hochschule, im Rahmen einer Kooperation, kommerzieller Provider) und dezentralem Cloud Management (auf dem eigenen Campus)

- Poolen von Verhandlungsmacht auf möglichst hohen Abstraktionsebenen, was zudem eine bessere juristische und fachliche eigene Position erwarten lässt; explizite Einflussnahme auf gestaltbare rechtliche Rahmenbedingungen (z.B. ADV-Verträge)

- Erkennen von Bedarfen – Kooperation zwischen Hochschulen, was die Beratungsangebote angeht: Wo wird und kann Expertise aufgebaut werden? Expertenzentren müssen nicht unbedingt pro Hochschule entstehen.

- Dual- bzw. Multi-Vendor Strategie befolgen und geeignete Anbieter auswählen. Definition von akzeptablen Bruchlinien in der Service-Integration, d.h., wo erscheint es mit Kompromissen realistisch, Angebote mehrerer Anbieter zu vertretbarem Mehraufwand zu mischen.

- Bestimmung einer Person/Instanz für die Begleitung der Cloud-Strategie auf Leitungsebene: Diese Funktion könnte bspw. am CIO aufgehängt sein.

- Aufgabenverteilung IT: Zukünftige dezentrale IT sollte deutlich stärker auf die (fachliche) Anwendungsebene des IT-Service-Stacks fokussieren, während die zentrale IT die Planungs- und Support-Kapazitäten auf die Basisebenen abhebt.

- Abstimmen eines einheitlichen Vorgehens beim Umgang mit Cloud-Anfragen aus nachgeordneten Einheiten, wie Fakultäten oder Professuren (z.B. durch Einrichtung eines User Boards)

- Entwicklung einer Strategie bzw. von Dokumenten für den Umgang mit „schwierigen“ Angeboten (z.B. End of Privacy Shield, Exportkontrollrecht)

- Aufbau von Cloud-Know-how und Personalressourcen „rund um“ die IT: Datenschutz, Recht, Beschaffung, …

- klare und regelmäßige Kommunikation zur eingeschlagenen Richtung: Definition einer klaren Aufgaben- und Rollenverteilung (für Fakultäten, Professuren, Projekte, RZs) sowie Delegation der Verantwortlichkeiten

- Etablierung zentraler Beratungs- und Support-Strukturen zum Thema Cloud: Bündelung von Know-how

- Entwicklung einer klaren Personalstrategie für den IT-Bereich sowie einer Strategie für die Aus- und Weiterbildung: Definition zukünftiger Qualifikationsprofile und entsprechende Bereitstellung von Weiterbildungen für verschiedene Zielgruppen (IT-Beauftragte, [IT-]Beschaffer, allgemeine Nutzende, Professorinnen und Professoren, Projekte …)

- Weitergabe der Erwartungen an Nachhaltigkeit (Energie, IT-Ressourcen)

- Nutzung von Berufungsverhandlungen zur internen IT-Steuerung; Forderungen zur besseren Skalierbarkeit eher mit „Sachleistungen“ (N CPU-Kerne in der Cloud, M RAM, L Storage) als mit Geld bedienen: Hierzu sollten sich Hochschulleitung, zentrale Beschaffung und IT-Dienstleister abstimmen, um angefragte Ressourcen geeignet zu bedienen.

- Bereitstellung eines Digital-Onboarding-Prozesses, der gleich eine Einführung in die Cloud-Nutzung in den gewünschten Aspekten beinhaltet

- Implementierung einer Governance für externe Dienstleistungen und Dienstanbieter

- Beförderung der gesellschaftlichen Diskussion und Entwicklung von Empfehlungen zur Rolle zentraler Software- und Cloud-Angebote, durch begleitende Forschung zu Digitalmärkten in den Wirtschaftswissenschaftlichen Fakultäten

- konsequente Risikobeurteilung im eigenen spezifischen Umfeld bzgl. Risiken und Chancen bei der Nutzung eines spezifischen Cloud-Angebots: Nur wenn der Nutzen größer ist und die Kosten für die Nutzung einer Cloud-Lösung die einer On-Premise-Lösung unterschreiten, sollte man sich für eine Cloud-Lösung entscheiden.

### 2.6.2. Empfehlungen für Rechenzentren

- Rolle und Aufgaben des Rechenzentrums gemeinsam mit der Hochschulleitung klären

- Beratung der Hochschulleitungen, was der Einsatz der Cloud (und vergleichbarer Technologien) bedeutet und wie man die Mittel hier sinnvoll kanalisiert (z.B. gewisse Vorleistung/Vorhalten bei Kapazitäten)

- Bereitstellen von Input für die Hochschulstrategie: Abwägung zwischen zentralem vs. dezentralem Cloud Management

- Abwägung zwischen verschiedenen Cloud-Ressourcen und Cloud-Modellen: kommerziell (bspw. für zukünftige Microsoft-basierte Office-Desktops, diverse Video-Conferencing-Lösungen als SaaS), eigene Ressourcen für Scientific Computing (inkl. Spezialangeboten wie HPC eher als IaaS)

- Exit-Strategie in einem Cloud-Konzept der Hochschule festhalten (z.B. Prozesse im RZ, Deployment Pipeline, Daten)

- vorausschauende Planung des Personalumbaus

- Abstimmung mit anderen RZs: Spezialisierung und Kooperation (Fokus auf bestimmte Dienste, die im eigenen Haus angeboten werden; Bestimmung der Dienste, die von extern bezogen werden)

- Koordination von IdM/AAI-Föderationen, Entwicklung gemeinsamer Konzepte und kompatibler Vorgehensweisen

- Anpassung der eigenen Ziele und Visionen an geänderte Realitäten und IT-Landschaft

- Schaffung von klaren Schnittstellen zur dezentralen IT (IT-Governance)

- explizite Einflussnahme auf gestaltbare (strategische) Rahmenbedingungen

- Forderung Nachhaltigkeit (Energie, IT-Ressourcen)

### 2.6.3. Empfehlungen für Fakultäten/Dekanate/Institute

- Fokussierung der Wissenschaft auf die eigenen Kompetenzen und nicht den generellen IT-Betrieb

- Planung des IT-Mitteleinsatzes im Spannungsfeld klassischer Projektkosten (Beschaffung einzelner Server, Software Stacks) vs. laufende Kosten von Cloud-Angeboten: Hier können Überlegungen bei Neuberufungen helfen.

- Strategie zur IT-Personalgewinnung und -weiterqualifizierung

# 3. Klärung der Rahmenbedingungen

*Vielfältige Rahmenbedingungen sind zu klären, bevor die ersten Schritte in der Cloud unternommen werden können. Hierzu zählen z.B. die Klassifikation von Daten sowie die Anforderungen aus Datenschutz und Informationssicherheit, aber auch rechtliche, vertragliche und technische Aspekte.*

Sobald die Entscheidung gefällt wurde, einen Cloud-Service an der Hochschule einzuführen, müssen zunächst die Rahmenbedingungen geklärt werden. Zu den Rahmenbedingungen gehören u.a.:

1. Identifikation der zu klärenden Fragestellungen
2. Identifikation der betroffenen Prozesse
3. Aufwandsabschätzung für die umzusetzenden Maßnahmen

Um diese Punkte vollumfänglich zu klären, müssen alle Beteiligten der Hochschule in einer dazu gehörigen Arbeitsgruppe eingebunden werden. Dazu gehören z.B. dezentrale und zentrale IT, Personalräte, Rechtsabteilung, Beschaffung, Datenschutzbeauftragte.

Um diese Rahmenbedingungen zu klären, empfiehlt es sich, diese zunächst exemplarisch für einen konkreten Cloud-Anbieter festzustellen und sich daran abzuarbeiten. Die so entstandenen Lösungen können in einem nächsten Schritt zu generellen Checklisten und Handreichungen ausgearbeitet werden, die anbieterunabhängig verwendet werden können. Beispiele dazu können sein:

- Einordnung: „Handelt es sich um eine Cloud-Beschaffung?“
- Checkliste für Cloud-Beschaffungen
- Verantwortlichkeiten und Rollen bei der Cloud-Nutzung (Nutzende, Institutsleitung, zentrale IT, Administratoren eines Instituts etc.)
- Hilfestellungen und Indikatoren zur Beantwortung der Frage: „Wann darf/soll ich die Cloud nutzen?“

## 3.1. Klassifikation von Daten & Cloud-Workflows

*Zielgruppe: Rektorate (hier insbesondere DSB, ISB), Rechenzentren, Fachbereiche*

Die Art der zu verarbeitenden Daten und angestrebte Workflows oder der Umfang einer Nutzergruppe für ein bestimmtes Cloud-Angebot sollten einer Abwägung unterzogen werden. So sollten insbesondere unkritische Forschungsdaten

1. ohne Personenbezug,
2. ohne leicht zu extrahierendes geistiges Eigentum und/oder
3. aus Kooperationen ohne besondere Anforderungen an die Vertraulichkeit

zügig behandelt werden. Das vereinfacht den Fokus auf Daten mit Personenbezug, geistigem Eigentum und/oder aus Industriekooperationen, für die stärkere Abwägungen zu treffen wären. Ebenso könnten Cloud-Angebote für kleine Gruppen – bezogen auf die Gesamtpersonenzahl einer Einrichtung (Forschende, Studierende, Verwaltung) – im Vergleich als deutlich unkritischer eingestuft werden als Angebote, die bspw. den Desktop eines wesentlichen Anteils einer Personengruppe (komplette Verwaltung, Standard-Desktop der Forschenden oder Mitarbeitenden in Lehrstühlen, Software-Umgebungen für Studierende) adressieren. Bei Letzteren sind langfristige Pfadabhängigkeiten deutlich höher und durch große Anzahlen kostspieliger als in kleinen, abgegrenzten Gruppen.

## 3.2. Anforderungen des Datenschutzes und der Informationssicherheit

*Zielgruppe: Rektorate (hier insbesondere DSB, ISB), Rechenzentren*

### 3.2.1. Informationssicherheit

#### Anforderungen an den Cloud-Anbieter

Nach der Erarbeitung der Cloud-Strategie, der Beschreibung der gewünschten Dienste in der Cloud und dem Erstellen eines Informationssicherheitskonzepts stehen Hochschulen vor der Wahl, einen geeigneten Cloud-Anbieter entsprechend der Cloud-Strategie auszuwählen[5]. Für die Feststellung der Eignung eines Cloud-Anbieters unter dem Gesichtspunkt der Informationssicherheit müssen folgende Fragen bei der Erstellung eines Lastenheftes bzw. einer Leistungsbeschreibung einfließen:

- Besitzt der Cloud-Anbieter nachweisbare Referenzen und damit eine entsprechende Reputation?
- Wird der Cloud-Anbieter in Ranglisten oder Bewertungsmatrizen von möglichst unabhängigen Organisationen geführt?
- Ist Cloud Computing das Kerngeschäft des Anbieters?[6]
- Welche Zugriffe durch den Cloud-Anbieter oder Dritte werden erlaubt oder sind möglich? An welchen Standorten (Rechenzentren, Ländern) werden die Informationen verarbeitet und gespeichert?
- Welches geltende Recht liegt dem Vertrag zugrunde, welchen rechtlichen Rahmenbedingungen unterliegt der Anbieter oder dessen Subunternehmer?

[5] Im Hochschulbereich gibt es hochschulübergreifende kooperativ angebotene Cloud-Dienste, die „Sync & Share“-Lösungen, webbasierte Office-Anwendungen und Kollaborationsplattformen anbieten. Bei diesen sind die spezifischen Anforderungen von Forschung, Studium und Lehre sowie Verwaltung bzgl. Informationssicherheit und Datenschutz regelmäßig berücksichtigt.

[6] wenn nein, besteht die Gefahr der Einstellung des Dienstes oder der Übernahme des Anbieters

- Beauftragt der Anbieter Subunternehmen zur Erbringung seiner Dienste?[7]

- Existiert ein Prüfbericht mit einem Testat eines unabhängigen Wirtschaftsprüfers, das sicherstellt, dass Kundenanforderungen eingehalten werden und Angaben zu Umfeldparametern des Cloud-Dienstes richtig sind?[8]

- Wurden die Dienste des Anbieters zertifiziert (z.B. ISO/IEC 27001)? Decken Gültigkeitsbereich (Scope) und die Erklärung der Anwendbarkeit (SOA) die Standorte der Datenverarbeitung und die Dienste ausreichend ab? Gibt der Anbieter diese Dokumente und die entsprechenden Nachweise (oder ggf. eine hinreichende Stichprobe davon) vor Vertragsabschluss heraus?

### Risiken

Die Nutzung von Cloud-Anbietern kann je nach Nutzungsgrad dieser Dienste unterschiedliche Auswirkungen auf die Informationssicherheit haben. Je höher der Nutzungsgrad ist und je mehr intern genutzte IT-Dienste in die Cloud verlagert werden, desto folgenschwerer sind Verletzungen der Informationssicherheit und desto mehr Gefährdungspotenzial besteht. Somit ergeben sich bei zunehmenden Nutzungsgrad höhere Anforderungen an die Informationssicherheit.

Die Auslagerung von Diensten in die Cloud macht Investitionen in Kontrollen zur Vermeidung interner Schwachstellen (wie mangelnde Planung, unzureichende Regelungen und Kontrollen) und externer Bedrohungen (wie Ausfall, Offenlegung von Informationen) notwendig. Ohne derartige Maßnahmen kann ein Dienst nicht sicher genutzt werden. Erschwerend kommt hinzu, dass diese Maßnahmen vertraglich mit dem Cloud-Anbieter verhandelt werden müssen und nicht hochschulintern bestimmt werden können.

### Chancen

Eine Cloud-Infrastruktur kann bei erhöhten Verfügbarkeitsanforderungen und Personalverfügbarkeit (wie Support, Betrieb) Vorteile generieren, wenn Dienste ausreichend beschrieben und detailliert vertraglich vereinbart werden. Bei den Kostenüberlegungen (Make or Buy) sollten die Frage „Wie viel Sicherheit möchte ich aus der Hand geben?“ und die zugehörigen Anforderungen des BSI[9] überprüft werden. Eine Implementierung von IT-Sicherheitsanforderungen oder Zertifizierungen sind für den Cloud-Anbieter oft leichter und effizienter umzusetzen bzw. werden bereits mit angeboten. Dies birgt im Gegenzug das Risiko einer unzureichenden Planung oder Steuerung dieser Anforderungen.[10]

---

[7] Frage dient zur Beurteilung von Abhängigkeiten

[8] z.B. SOC2 Testat; zu beachten ist, dass ISO-Zertifikate gegenüber Testaten (SOC2, C5) vorzuziehen sind, weil Zertifikate einem normierten Prüfprozess unterliegen.

[9] BSI IT-Grundschutz-Kompendium, OPS.2.2 Cloud-Nutzung, inkl. Umsetzungshinweise

[10] siehe ISO 27001 – A.15 Lieferantenbeziehungen

### 3.2.2. Datenschutz

#### Anforderungen an den Cloud-Anbieter

Im Rahmen der Cloud-Strategie ist zunächst zu prüfen, für welche Verfahren bzw. Geschäftsprozesse aus Forschung, Lehre und Verwaltung mit personenbezogenen Daten externe Cloud-Anbieter in Anspruch genommen werden sollen oder können (vgl. Kapitel 3.1). Sofern noch nicht erfolgt, ist zu bewerten, wie schutzwürdig die Daten aus Sicht der betroffenen Personen sind (Daten-/Informationsklassifizierung). Je höher die Schutzwürdigkeit der Daten ist, umso höher sind die datenschutzrechtlichen Anforderungen an den Cloud-Anbieter. Für bestimmte Datenverarbeitungsvorgänge – bspw. die Verarbeitung besonderer Kategorien personenbezogener Daten – kann es sogar möglich sein, dass der Einsatz eines Cloud-Anbieters durch spezifische Bestimmungen nur eingeschränkt möglich bzw. sogar gesetzlich untersagt ist.

Zudem sind bei einer Datenübermittlung außerhalb der EU und des EWR (internationaler Datentransfer), wie etwa der Verarbeitung von personenbezogenen Daten in den Vereinigten Staaten von Amerika bzw. bei entsprechenden Zugriffsmöglichkeiten von Dienstleistern aus Drittländern für Support- oder Service-Dienstleistungen (bspw. zu Wartungszwecken), zahlreiche weitere rechtliche Anforderungen zu beachten, um sicherzustellen, dass das in der EU gewährleistete Schutzniveau nicht untergraben wird.

Hochschulen dürfen als datenschutzrechtlich Verantwortliche nur mit solchen Cloud-Anbietern zusammenarbeiten, die hinreichend Garantien dafür bieten können, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist[11]. Für die Feststellung der Eignung eines Cloud-Anbieters unter dem Gesichtspunkt Datenschutz sind deshalb insbesondere – nicht abschließend – folgende Mindestanforderungen zu stellen und (regelmäßig) zu überprüfen:

- transparente und eindeutige vertragliche Regelungen zur weisungsgebundenen Verarbeitung der Daten beim Cloud-Anbieter, insbesondere zum Gegenstand und zur Dauer der Verarbeitung, zur Art und zum Zweck der Verarbeitung, zur Art der personenbezogenen Daten, zur Kategorie betroffener Personen, zu Pflichten und Rechten der Hochschule, zu den Orten der Datenverarbeitung und zu der Frage, welche Maßnahmen (Art. 44 ff. DSGVO) bei internationalen Datentransfers ergriffen werden

- detaillierte und prüfbare Informationen über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der Dienstleistungen des Cloud-Anbieters

- aktuelle und aussagekräftige Nachweise (bspw. Zertifikate) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird

[11] vgl. Art. 28 Abs. 1 DSGVO: „Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet."

#### Risiken

Die Hochschule als datenschutzrechtliche Verantwortliche haftet für den Schaden, der durch eine nicht der Datenschutz-Grundverordnung entsprechende Datenverarbeitung verursacht wurde. Dagegen haftet ein Cloud-Anbieter nur, wenn er seinen speziellen Pflichten als Auftragsverarbeiter nicht nachgekommen ist. Dazu zählt vor allem die Nichtbeachtung der rechtmäßig erteilten Anweisungen des Verantwortlichen. Gerade bei der zunehmenden Digitalisierung und Komplexität von IT-Dienstleistungen sowie dem zunehmenden Einsatz von marktstarken Cloud-Anbietern ist es für die einzelnen Hochschulen äußerst schwierig, die o.g. Anforderungen prüfen bzw. nachweisen zu können und ggf. vertragliche bzw. technische Anpassungen zu erreichen, um diesen Haftungsrisiken entgegenzuwirken und den vollumfänglichen Schutz der personenbezogenen Daten zu gewährleisten. Dies kann am effizientesten nur erreicht werden, wenn die Hochschulen über Kooperationen gemeinsame Prüfmechanismen etablieren.

Weitere Risiken können sich ergeben, wenn der Cloud-Anbieter Zugang zu besonders schutzwürdigen personenbezogenen Daten erhält (z.B. zu Gesundheitsdaten) oder die personenbezogenen Daten unsachgemäß entgegen der erteilten Weisungen zu eigenen Zwecken (weiter-)verarbeitet.

#### Chancen

Die Nutzung von Cloud-Diensten kann über die Chancen, die im Hinblick auf die Informationssicherheit genannt wurden, auch zu einem effektiveren Datenschutz führen, wenn bspw. der Cloud-Anbieter bzgl. der technischen Maßnahmen zur sicheren Verarbeitung von personenbezogenen Daten ein höheres Schutzniveau und geschultes Personal vorweisen kann, als dies in der Hochschule mit eigenen Ressourcen leistbar wäre.

## 3.3. Beschaffung

*Zielgruppe: Verantwortliche für die Beschaffung,*
*z.B. in Rechenzentren und der Hochschulverwaltung*

Für die Beauftragung von Cloud-Angeboten müssen klare Abläufe für die Beschaffung und Buchung von Cloud-Diensten unter Berücksichtigung der vorhandenen Prozesse zur Beschaffung von Software und Hardware etabliert werden. Zu klärende Fragen sind z.B., was zentral beschafft und verwaltet werden soll und was dezentral beschafft werden kann. Welche zentralen Strukturen werden hier benötigt und welche Kompetenzen? (vgl. Kapitel 2.4.)

### 3.3.1. Zentrale Organisation für große „Vendor“

Bei Lösungen, deren Einsatz in der ganzen Hochschule oder in weiten Teilen zu erwarten ist, sollte eine zentrale Einheit der Hochschule für die Einführung und damit auch die Organisation und Beschaffung zuständig sein. Je nach Organisation der Hochschule kann das z.B. die zentrale IT oder die zentrale Beschaffungsstelle sein (sofern vorhanden).

Das hat folgende Vorteile:

- Know-how für Cloud-Beschaffungen wird zentral aufgebaut: Da bei den meisten Verträgen ähnliche Punkte zu prüfen sind, kann man hier Synergieeffekte nutzen. In Summe wird dadurch der Aufwand verringert.

- Die Einführung kann zentral organisiert werden, was z.B. die technische Anbindung des Anbieters an die Hochschulstrukturen erleichtert (siehe Kapitel 3.7.).

- Die Einbindung von hochschulweiten Gremien (z.B. Personalräte, Datenschutzbeauftragte, Rechtsabteilung) ist einfach möglich.

- Die Hochschule hat einen besseren Überblick über die genutzten Ressourcen.

- Es können möglicherweise Preisreduzierungen verhandelt werden.

Zu klären ist der Aspekt, wie Anforderungen der einzelnen Nutzenden oder von Bezugsgruppen diese zentralen Stellen erreichen. Schon vorhandene zentrale Strukturen für z.B. hochschulweiten Support erleichtern hier auf jeden Fall den Weg. Die Empfehlung ist hier, einen Workflow für diese Beschaffungen festzulegen und durch offensive Öffentlichkeitsarbeit zu kommunizieren.

### 3.3.2. Überlegungen für kleinere Lösungen

Die Hochschule kann gemeinsam mit der zentralen IT und der Beschaffungsstelle festlegen, wo Einrichtungen/Nutzerinnen und Nutzer an der Hochschule eigenständig Lösungen abrufen können. Auch hier gelten die o.g. Punkte (siehe Kapitel 3.3.1), bspw. kann die zentrale Stelle vorher die kleinen Angebote den Gremien zur Mitbestimmung vorgelegt haben.

Es kann festgelegte kleine Lösungen geben, aber auch Unterlagen können bereitgestellt werden (bspw. eine Checkliste: Vergleichsangebote, Datenschutz, Personalräte, Beschaffungsrichtlinien, Kommunikationskanäle festlegen/Angebot streuen), damit Bereiche selbstständig Angebote jenseits dieser Lösungen beschaffen können. Die Hochschule sollte festlegen, wofür die zentralen Stellen zuständig sind und was unter großen und kleinen Lösungen zu verstehen ist. Eine Beratung durch die zentrale IT (oder IT-Beschaffung) kann als Zusatzangebot nützlich sein.

### 3.3.3. Hochschulübergreifende Kooperationen

Bei zentralen Komponenten mit weiter Verbreitung lohnt sich die Betrachtung einer hochschulübergreifenden Beschaffung (z.B. Zoom), um sowohl gegenüber dem Anbieter eine bessere Verhandlungsposition zu haben als auch in Summe Ressourcen für die Beschaffung und Kompetenzen zur Lizenzverwaltung zu bündeln.

## 3.4. Vertragliche Anforderungen

*Zielgruppe: Verantwortliche für die Beschaffung,*
*z.B. in Rechenzentren und der Hochschulverwaltung*

Um Cloud-Produkte nutzen zu können, müssen diese in den meisten Fällen explizit beschafft werden. Da die Beschaffung von Cloud-Produkten meist einige zusätzliche Fragen mit sich bringt, werden im Folgenden wichtige Aspekte erläutert.

### 3.4.1. Indikatoren für eine Cloud-Beschaffung

Um ein Verfahren zu entwickeln, wie mit Cloud-Beschaffungen umzugehen ist, müssen diese zunächst identifiziert werden. Folgende Hinweise deuten auf eine Cloud-Beschaffung hin (müssen aber nicht alle immer erfüllt sein!):

- Es muss keine Software lokal installiert werden.
- Rechenleistung wird über ein externes Rechenzentrum (= nicht auf dem Gelände der Hochschule) zur Verfügung gestellt.
- Lokal installierte Software wird durch Cloud-Speicher oder Cloud-Dienste ergänzt oder erfordert eine Cloud-basierte Nutzer- und/oder Lizenzverwaltung.
- Die Miete der Software/des Service erfolgt für einen bestimmten Zeitraum.

### 3.4.2. Vergaberechtliche Vorgaben

Neben den rechtlichen Regelungen, die bei jeder Beschaffung gelten, gibt es auch eine Reihe von Empfehlungen und Vorgaben, die sich explizit auf Cloud-Dienste beziehen:

- Vorgaben des Rechnungshofs[12]
- Vorgaben des IT-Planungsrats[13]
- BSI-Grundschutz[14]
- Geheimhaltung/Geheimnisschutz[15]
- ggf. Rechtsgutachten des DFN

### 3.4.3. Auswirkungen des (US-)Exportkontrollrechts

Die Bereitstellung von Wissen/Know-how oder Technologien in einer Cloud stellt dann einen Export dar, wenn auch Personen aus dem Ausland Zugriff auf diese Inhalte erhalten oder die Daten auf Servern außerhalb Deutschlands gehostet werden. Der Austausch von bereits allgemein zugänglichen Informationen ist unkritisch. Für den grenzüberschreitenden Austausch der Inhalte, die in der Cloud

[12] https://www.bundesrechnungshof.de/de/veroeffentlichungen/produkte/weitere/leitsaetze-fuer-die-pruefung-von-iuk-outsourcing

[13] https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/21_Sitzung/14_Anlage1_Cloud-Computing.pdf;jsessionid=A3461FB7C3BEEC1E521DBBC4A5908C2A.1_cid332?__blob=publicationFile&v=2

[14] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/cloud-computing_node.html

[15] https://www.bitkom.org/Bitkom/Publikationen/Muster-zur-Umsetzung-des-Gesetzes-zur-Neuregelung-des-Schutzes-von-Geheimnissen-bei-der-Mitwirkung-Dritter-an-der-Berufsausuebung-schweigepflichtiger-Personen.html

abgelegt sind, müssen somit auch außenwirtschaftsrechtliche Genehmigungspflichten oder Verbote beachtet werden.

Um das Risiko hier möglichst gering zu halten, empfehlen wir folgende Maßnahmen:

- Serverstandort der Cloud-Dienstleistung sollte ausschließlich Deutschland sein (mind. Europa).
- Prüfen: Wer bekommt Zugriff auf die Daten? Gibt es ggf. Nutzende außerhalb von Deutschland (Support? Subunternehmen?)?
- Sollten mehrere Projekte der Hochschule beim selben Cloud-Anbieter gehostet werden (wie z.B. bei der Nutzung von Azure oder AWS), so sollten die Projekte separiert sein und kein Zugriff untereinander bestehen.
- Prüfung von sogenannten Sanktionslisten wie www.finanz-sanktionsliste.de vor der Freigabe von Daten an Externe
- Prüfung von Länderembargos[16] vor der Freigabe von Daten an Externe
- Vorgabe an die Nutzenden, dass, wenn kritisches Wissen oder Technologien über einen Cloud-Anbieter einer Person aus dem Ausland zur Verfügung gestellt werden sollen, dies im Zweifel mit der zuständigen Abteilung für Zoll der eigenen Hochschule abzusprechen ist.

### 3.4.4. Vertragsunterlagen

Neben den rechtlichen Voraussetzungen muss auch noch eine Reihe weiterer Aspekte im Vertrag geprüft werden, um eine konforme Nutzung zu gewährleisten:

- Wer (oder welche Nutzergruppe) darf welche Dienstleistungen/Produkte aus dem Vertrag nutzen?
- Gibt es Regelungen zur privaten Nutzung? Entstehen dadurch ggf. steuerliche Probleme durch geldwerten Vorteil?
- Gibt es Unterschiede in der Online-/Offline-Nutzung bzw. bei lokalen Installationen?
- Gibt es Einschränkungen, welche Arten von Daten verarbeitet werden dürfen (bspw. personenbezogene Daten Dritter)?
- Gibt es Regelungen für hybride Nutzungsrechte, z.B. bzgl. der Lizenzierung?
- Was passiert mit den Daten bei Vertragsende?

[16] https://www.zoll.de/DE/Fachthemen/Aussenwirtschaft-Bargeldverkehr/Embargomassnahmen/Laenderembargos/laenderembargos_node.html

## 3.5. Lizenzierung

*Zielgruppe: Verantwortliche für die Beschaffung und Verwaltung von Lizenzen in Rechenzentren und der Hochschulverwaltung*

Im Vorfeld sollten Bezahl-/Abrechnungsmodalitäten sowie Lizenzierungsmöglichkeiten mit der Zentralen Beschaffung/dem Finanzdezernat o.Ä. und den einzelnen Einrichtungen der Hochschule besprochen werden, um Besonderheiten zu klären. Gemeinsam mit dem Cloud-Anbieter sollte eine geeignete Lizenzierungs- und Abrechnungsstruktur erarbeitet werden (vgl. Kapitel 3.36.).

Bei der Lizenzierung ist auf die Lizenzierungsbasis zu achten: Während SaaS-Produkte meist nach der Zahl der Nutzenden abgerechnet werden, gelten bei PaaS oder IaaS andere Abrechnungseinheiten. Die Infrastruktur für Lizenzierung und Abrechnung sollte vor der Beschaffung mit dem Cloud-Anbieter und den Beteiligten an der Hochschule diskutiert und festgelegt werden. Grundsätzlich ist darauf zu achten, ob je nach Lizenzierung z.B. weitere Rabattmodelle mit dem Cloud-Anbieter zu verhandeln sind. So kann es z.B. bei einer Lizenzierung nach der Zahl der Nutzenden von Vorteil sein, eine hochschulweite Lizenz zu erwerben, um in Summe Kosten zu sparen. Hierbei sollte man aufpassen, dass wegen der Attraktivität der sinkenden Kosten pro Client auf Multi-Vendor-Strategien verzichtet wird, um den Kostenrahmen einzuhalten.

Bei der Lizenzierung gibt es meist zwei verschiedene Ansätze:

- Nutzerbasierte Lizenzierung: Hier fällt pro Nutzenden eine Lizenz an, die je nach Umfang auch unterschiedlich ausgeprägt sein kann. Diese Art der Lizenzierung findet sich häufig bei SaaS-Angeboten.

- Gerätebasierte Lizenzierung: Hier fällt pro (virtuellem) Gerät/Einheit eine Lizenz an. Diese Art der Lizenzierung findet sich meist bei PaaS oder IaaS.

Die vereinbarte Lizenzierung muss in der technischen Anbindung umgesetzt werden, z.B. durch die Bildung geeigneter Nutzergruppen und die Zuweisung unterschiedlicher Lizenzen (siehe Kapitel 3.7.1.). Die ggf. anfallenden Kosten müssen vom Abrechnungsmodell des Cloud-Anbieters übertragen und in den eigenen Abrechnungsmodellen abgebildet werden. Die Technik ist bspw. dann involviert, wenn ein Anbieter Kosten einem Cloud-Konto zuordnet, die nur die Technik (z.B. das lokale IdM-System) einem Mitarbeitenden zuordnen kann. Ggf. beeinflussen die Anforderungen zur Abrechnung die Abbildung der eigenen Strukturen in der Cloud, indem z.B. Mandanten nicht nach rein organisatorischen Gesichtspunkten zugeordnet werden können, sondern Grundlage für die Kostenumlage abbilden müssen.

## 3.6. Abrechnung

*Zielgruppe: Verantwortliche für die Beschaffung und Abrechnung (z.B. für Software und Hardware) in Rechenzentren und der Hochschulverwaltung*

Im Vertrag mit dem Cloud-Anbieter wird meist direkt auch die Art der Abrechnung geregelt. Ob diese nun nutzungsbasiert erfolgt (z.B. „verbrauchte CPU-Stunden“ bei IaaS-Angeboten oder „belegter

Speicherplatz“) oder nur Lizenzkosten anfallen, am Ende muss die Abwicklung und Bezahlung einer Rechnung geregelt werden.

Bei der Rechnungsstellung sollte innerhalb der Hochschule geprüft werden, auf welcher Basis die Abrechnung benötigt wird, sodass die über die Cloud angefallenen Kosten bestmöglich abgerechnet werden können. Dabei gibt es grundsätzlich verschiedene Ansätze:

- Jedes Institut/Projekt erhält eine dedizierte, steuerrechtlich relevante Rechnung: So werden die Kosten direkt dort in Rechnung gestellt, wo sie entstehen.
- Die Rechnung geht an eine zentrale Stelle und wird von dort zentral bezahlt. Die Aufteilung auf Institute/Projekte erfolgt hochschulintern durch Umbuchungen. In diesem Fall muss es möglich sein, eine konkrete Zuordnung zu Nutzenden/Projekten und/oder Instituten vorzunehmen.

In beiden Fällen werden Verwaltungsmechanismen benötigt, die Lösungen ermöglichen:

- Wie ist das Unterscheidungsmerkmal, das für die Rechnungsgenerierung genutzt wird? Wie kommt der Cloud-Anbieter an die korrekte Rechnungsadresse? Werden hierdurch Mehrkosten verursacht?
- Wer kommt zunächst für die Kosten auf? Wie können die Kosten konkreten Konten zur Umbuchung zugeordnet werden? Wer übernimmt den zusätzlichen Aufwand zur Rechnungsaufteilung und Umbuchung?

Daneben sollten folgende Punkte im Vorfeld mit dem Cloud-Anbieter geklärt und festgelegt werden:

- Abrechnungsperiode: monatlich, quartalsweise, jährlich?
- Wahl des Bezahlmodells: „Pay as you go“ vs. Prepaid, Kreditkarte vs. Rechnung
- Kostenkontrolle/Klärung der Einsicht in generierte Kosten: Wie kann man die bisher generierten Kosten einsehen, um die monatliche Nutzung abzuschätzen?
- (Wie) können Kosten gedeckelt werden? Kann man bezogen auf Universität, Institut oder einen einzelnen Lehrstuhl Limits einrichten? (Eine einzige vergessene virtuelle Maschine kann durchaus 2.000 US$ im Monat kosten.)

## 3.7. Anforderungen der technischen Anbindung

*Zielgruppe: Entscheider sowie Verantwortliche für die technische Umsetzung.*

Bei der Anbindung eines Cloud-Anbieters gibt es eine Reihe von Prozessen, die anbieterunabhängig zu betrachten sind. Ziel ist es, die vorhandenen Prozesse der Hochschule technisch so an die Lösung des Anbieters anzubinden, dass möglichst wenig angepasst werden muss. Folgende Prozesse bzw. Fragestellungen sind dabei zu beachten:

- Nutzerprovisionierung: Wie können die Daten der Nutzenden aus der Hochschule gezielt zum Cloud-Anbieter übertragen werden und worauf muss man hier achten?

- Authentifizierung: Wie kann man die Authentifizierung der Nutzenden möglichst einfach und sicher ermöglichen?
- Netzwerk: Müssen die Cloud-Anwendungen eine Anbindung ans Hochschulnetz haben? Welche Vor- und Nachteile hat das und was ist dabei zu beachten?
- Administration/Strukturierung

Ob alle Punkte für die Anbindung eines Cloud-Anbieters relevant sind oder nur Teilaspekte davon, hängt davon ab,

- welche Teile der Hochschule den Dienst nutzen: je größer die Anzahl der Nutzenden, desto mehr sollte zentral geregelt werden;
- welche Art von Cloud Dienst genutzt wird;
- welche Daten zur Nutzung des Dienstes notwendig sind

Im Bereich der technischen Anbindung liegt zunächst ein Schwerpunkt auf SaaS. Das ist dem besonderen Interesse an Diensten wie Microsoft 365 (Teams) oder Videokonferenzplattformen (Zoom, ...) geschuldet, die in diesen Bereich fallen. Die meisten Erkenntnisse (z.B. für den Bereich Nutzerprovisionierung oder Authentifizierung) gelten aber für IaaS und PaaS gleichermaßen.

Die folgenden Unterkapitel sollen dem fortgeschrittenen Leser mit entsprechenden Fachkenntnissen einen Überblick über das Thema, Lösungsalternativen, besondere Herausforderungen etc. geben. Sofern möglich, wird auf externe Quellen und Anleitungen verwiesen, es ist kein Ziel der ZKI-Kommission, eigene Anleitungen zu erstellen oder zu pflegen.

### 3.7.1. Nutzerprovisionierung

Die gezielte Provisionierung von Nutzenden(-daten) durch die Hochschule an den Cloud Provider ermöglicht, den Datenfluss gezielt zu steuern. Das hat folgende Vorteile:

- Umsetzung eines Lifecycles
- Auswahl der Attribute zur Übertragung
- Steuerung von Berechtigungen und Lizenzen
- Bildung von Gruppen aufgrund von Merkmalen aus der Hochschulorganisation (z.B. Mitarbeitende und Studierende)

Im Folgenden werden die konkret zu implementierenden Prozesse erläutert.

#### Klärung der zu übertragenden Gruppen

Es sind vielfältige Kriterien denkbar, nach denen die Nutzenden eines Cloud-Dienstes eingeschränkt werden können/müssen, z.B. vor dem Hintergrund des Datenschutzes (alle Nutzenden, nur Nutzende mit Zustimmung zur Cloud-Nutzung, ...) oder der Lizenzierung (Campus-Lizenz für alle, nur Lizenzen zur Nutzung in der Lehre, ...).

Zunächst ist die Bildung dieser Gruppe(n) mit den beteiligten Stakeholdern (Datenschutzbeauftragte etc.) zu klären und (z.B. im lokalen IdM-System) umzusetzen. Dabei sind auch Fälle zu berücksichtigen, wenn ein Nutzender die Voraussetzungen nicht länger erfüllt (Widerruf der Zustimmung; nicht länger in der Lehre tätig, ...) und entsprechend eine Deprovisionierung eingeleitet werden muss.

### Explizites Einverständnis vs. automatische Übertragung von Nutzenden

Zunächst ist zu klären, ob die Daten aller potenziellen Nutzenden automatisch an den Cloud-Anbieter übertragen werden sollen oder im Vorfeld ein explizites Einverständnis für die Datenübertragung notwendig ist. Dies hat in Rücksprache mit dem/der Datenschutzbeauftragten zu erfolgen. Zu berücksichtigen ist hier, ob die getroffene Regelung dann für alle (potenziellen) Cloud-Anbieter gilt oder jedes Mal neu entschieden werden muss. Sofern Zustimmungen erforderlich sind, ist dafür ein Verfahren vorzubereiten, z.B. in Form eines Self-Service-Formulars.

### Anlegen, ändern, löschen von Nutzendendaten

Neben dem Anlegen von neuen Nutzenden durch die gezielte Nutzerprovisionierung muss auch die Änderung von übertragenen Daten sowie ein gezieltes Löschen von Nutzendendaten möglich sein. Dadurch können z.B. hochschulinterne Prozesse (z.B. Namensänderungen; Studierender wird Mitarbeitender; Studierender verlässt die Hochschule) automatisch in die Cloud übertragen werden. Um das vollumfänglich zu ermöglichen, ist es sinnvoll, dass die Nutzerprovisionierung aus einer Quelle erfolgt, die möglichst alle notwendigen Daten vollumfänglich enthält (z.B. ein Identity-Management-System).

### Übertragung von Attributen

Die genauen Attribute, die übertragen werden (müssen), unterscheiden sich je nach Cloud-Anbieter. Umfang und Belegung der Attribute sind in der Regel mit dem Datenschutz oder anderen Gremien der Hochschule (z.B. Personalräte) zu klären.

Hierbei sollte auch die Art der Nutzung des Dienstes berücksichtigt werden. Für Kollaboration ist z.B. ein Klarname unerlässlich, für andere Dienste wiederum eine anonyme oder pseudonyme Nutzung möglich.

Passwörter sollten nicht in die Cloud übertragen werden (siehe Kapitel 3.7.2.).

### Steuerung von Berechtigungen und Lizenzen

Durch die Nutzung der Informationen aus den Hochschulsystemen ist es möglich, die Nutzung der Cloud-Dienstleistungen besser zu steuern, z.B.:

- Verteilung von Lizenzen: Basierend z.B. auf dem Status eines Nutzenden (Mitarbeitender, Studierender) ist es möglich, gezielt Lizenzen zuzuweisen.
- Verteilung von Berechtigungen: Nutzt man weitere Daten, wie z.B. organisatorische Zuordnung oder Rollen innerhalb der Hochschule, ist es möglich, auch Berechtigungen in der Cloud daran anzulehnen. Das kann z.B. genutzt werden, um Berechtigungen für die Generierung von Kosten zu vergeben oder organisatorische Strukturen (ähnlich wie Mandanten) in der Cloud abzubilden.

### 3.7.2. Authentifizierung

Die konkrete Art der Authentifizierung ist stark abhängig vom Cloud-Anbieter und auch von der lokalen IdM-Strategie der Hochschule. Hierbei gibt es drei grundsätzliche Möglichkeiten:

- Die Möglichkeit einer Anmeldung über SAML ist verbreitet und ermöglicht die Nutzung der lokalen Authentifizierungsinfrastruktur (z.B. Shibboleth), ohne Übertragung der Credentials.
- Synchronisierung der lokalen Credentials (Benutzername und Passwort) zum Cloud-Anbieter
- Nutzung von „cloud only“ Credentials, die direkt beim Cloud-Anbieter generiert werden

Bei der Auswahl des Verfahrens müssen neben der technischen Machbarkeit auch folgende Aspekte betrachtet werden:

- Sicherheit: Dürfen die Passwörter in die Cloud synchronisiert werden? Was passiert, wenn die Passwörter lokal oder in der Cloud kompromittiert werden?
- Abhängigkeit: Je nach gewählter Authentifizierung ist die Nutzung von Cloud-Diensten abhängig von lokalen Authentifizierungsinfrastrukturen.
- Usability: Wie komfortabel funktioniert die Authentifizierung aus Sicht des Nutzenden?
- Support-Prozesse: Welche Support-Strukturen bzw. Selfservice-Prozesse für den Verlust von Credentials gibt es?

### 3.7.3. Netzwerk

Gerade bei IaaS und PaaS sollte das Thema Netzwerk in der Cloud mit genauso viel Sorgfalt betrachtet werden wie das lokale Hochschulnetz. Bevor Services in die Cloud migriert werden, sollten auch hier Aspekte wie Datenflüsse, Firewall und Netzwerkstrukturen geklärt werden. Hier sind in jedem Fall auch die lokalen Netzwerkadministratoren in die Gestaltung der Prozesse und Regelungen einzubeziehen.

#### Anbindung des Hochschulnetzes an die Cloud

Eine Anbindung des Cloud-„Rechenzentrums“ an das Hochschulnetz ist notwendig, wenn eine (dauerhafte) Übertragung von sensiblen Daten aus der Hochschule auf Systeme in der Cloud stattfinden soll.

*Achtung:* Durch die Anbindung von einem Cloud-Anbieter an das Hochschulnetz wird hier ggf. eine direkte Verbindung geschaffen, die auch potenzielle Angriffsvektoren mit sich bringt. Deswegen ist hier dann noch stärker auf die Absicherung der Anwendungen in der Cloud zu achten.

Je nach Cloud-Anbieter gibt es verschiedene Möglichkeiten der Anbindung (z.B. über VPN Tunnel, direkte ExpressRoute o.Ä.). Hier sollten auf jeden Fall die zuständigen Netzwerkexperten der Hochschule in die Planung und Umsetzung eingebunden werden.

#### Typisches Szenario

Bei einem IaaS-Anbieter werden mehrere virtuelle Instanzen gebucht, die in ein gemeinsames Netz des IaaS-Anbieters geschaltet werden. Diese Instanzen sollen dann auf interne Netze an der Hochschule zugreifen, z.B. über eine VPN-Koppelung.

### 3.7.4. Administration und Strukturierung

#### Kultur

Auch in der Technik haben sich in den unterschiedlichen Hochschulen verschiedene Kulturen entwickelt, die im Zusammenhang mit der Cloud-Nutzung berücksichtigt werden sollten.

Eine Hochschule mit einer starken zentralen IT wird sich ggf. leichter tun, Dienste in der Cloud zu betreiben. Bei einer dezentral aufgestellten IT (z.B. eigene IT-Abteilungen in den Fakultäten) wird man hingegen zusätzliche Anforderungen haben, diese Strukturen z.B. in Form von Berechtigungen/Rollen oder getrennten Mandanten in der Cloud umzusetzen. Dies sollte ggf. schon bei der Auswahl der Cloud-Anbieter berücksichtigt werden.

#### Erzwungene Änderungen

Große Cloud-Anbieter nehmen wenig Rücksicht auf einzelne Mandanten. Änderungsankündigungen erreichen teilweise zuerst die Technik und müssen sorgfältig auf die Auswirkungen auf den eigenen Mandanten hin überprüft und ggf. intern aufgearbeitet/kommuniziert werden. Dabei treibt der Zeitplan des Cloud-Anbieters ggf. die eigene Hochschule.

Ein subtil geändertes Design mag unkritisch sein, neue Analysefunktionen müssen hingegen zeitnah nicht nur in der Technik betrachtet, sondern ggf. auch vom/von der Datenschutzbeauftragen und weiteren Gremien bewertet werden. Es kann sich anbieten, für diesen Zweck einen festen Kreis zu etablieren.

#### Veränderte Aufgabenverteilung

Zum einen ist die Aufgabenverteilung zwischen Cloud-Anbieter und der Hochschule zu klären. Wer hilft dem Anwender, der Probleme bei der Nutzung des Cloud-Dienstes hat? Falls es SLAs gibt: Wer kann diese überprüfen und dokumentieren? Reicht das eigene Monitoring oder benötigt man externe Dienstleister?

Auch innerhalb der Hochschule können Aufgabenverteilungen infrage gestellt werden. Beispielsweise ist es denkbar, das Sharepoint Sites, Wikis oder E-Mail-Verteiler zentral durch die Technik eingerichtet werden mussten, der Cloud-Anbieter aber entsprechende Self-Services für alle Nutzenden anbietet. Dementsprechend ist zu prüfen, ob die bisherigen Prozesse beibehalten werden sollen oder Anpassungen möglich sind.

## 3.8. Empfehlungen

### 3.8.1. Empfehlungen für Hochschulleitungen

- Abstimmung mit „höheren“ Ebenen (Land, Bund) auch für ausreichende juristische Expertise

- Kanalisierung der Beschaffungen über eine zentrale Stelle, um Bedarfe zu verstehen und Bündelung zu ermöglichen
- Überblick über laufende Lizenzausgaben pro Anbieter, um Ressourcen besser bündeln zu können
- Integration der Abrechnung von Cloud-Produkten in die normalen Prozesse der Hochschule; Berücksichtigung von notwendigen Modellen z.B. bei geförderten Projekten
- Klassifikation von Daten und Cloud-Applikationen nach Kritikalität, sodass bei unkritischen Daten und eher kleinen Applikationen für eingeschränkte Nutzerkreise schnell und unkompliziert positiv beschieden werden kann
- Erstellung von Leitfäden zur Berücksichtigung der Rahmenbedingungen, z.B. in Form von Fragebögen, Checklisten, Nutzungsbedingungen
- Kooperation über Organisationen wie ZKI bzw. auch die HRK, insbesondere beim Einsatz von großen Cloud-Anbietern, um sich gegenüber Cloud-Anbietern gestärkt zu positionieren
- zentrale Organisation von Cloud-Beschaffungen für große „Vendor“
- Etablierung eines Workflows für Beschaffungen von Cloud-Produkten, der von einer zentralen Einheit der Hochschule überwacht wird.

### 3.8.2. Empfehlungen für Rechenzentren (bzw. zuständige Cloud-Administratoren)

- Bündelung von Lizenzen, möglichst große Rahmen, wie Bundes-, Landes-, Campuslizenzen
- Nutzung des lokalen IdM (sofern vorhanden) zur gezielten Provisionierung von Nutzenden und Daten
- Nutzung eines lokalen SSO-Systems für die Authentifizierung, i.d.R. SAML auf Basis Shibboleth; keine Übertragung von lokalen Credentials (Benutzername + Passwort) in die Cloud; 2FA, wo möglich
- Strategie zur Lizenzierung und Abrechnung
- Konzepte zur Netzwerkanbindung an das Hochschulnetz und allgemeinen Administration
- Berücksichtigung des vorhandenen Lifecycles eines Nutzenden (Anlegen, Ändern, Sperren, Löschen) auch in der Cloud

### 3.8.3. Empfehlung für beschaffende Einheiten

- Serverstandort der Cloud-Dienstleistung sollte ausschließlich Deutschland sein (mind. Europa)
- Prüfen: Wer bekommt Zugriff auf die Daten? Gibt es ggf. Nutzende außerhalb von Deutschland (Support? Subunternehmen?)?

- Sollten mehrere Projekte der Hochschule beim selben Cloud-Anbieter gehostet werden (wie z.B. bei der Nutzung von Azure oder AWS), so sollten die Projekte separiert sein und kein Zugriff untereinander bestehen.

- Prüfung von sogenannten Sanktionslisten wie www.finanz-sanktionsliste.de vor der Freigabe von Daten an Externe

- Prüfung von Länderembargos vor der Freigabe von Daten an Externe

- Vorgabe an die Nutzenden, dass, wenn kritisches Wissen oder Technologien über einen Cloud-Anbieter einer Person aus dem Ausland zur Verfügung gestellt werden sollen, dies im Zweifel mit der zuständigen Abteilung für Zoll der eigenen Hochschule abzusprechen ist.

# 4. Umsetzung der Rahmenbedingungen

*Zielgruppe: RZ-Leitungen bzw. Verantwortliche für die technische und organisatorische Umsetzung*

*Bei der Umsetzung der erarbeiteten Rahmenbedingungen ist eine umfassende Kommunikation in allen Belangen (inkl. Support, Dokumentation) notwendig, um diesen Change zu begleiten. Darüber hinaus ist genügend Zeit einzuplanen, z.B. durch einen mehrstufigen Einführungsprozess.*

## 4.1. Organisatorische Umsetzung

Die im Vorfeld erarbeiteten Anforderungen aus den organisatorischen Rahmenbedingungen müssen umgesetzt werden. Hierbei sind folgende Aspekte besonders zu beachten:

- Schulungen
- Dokumentation (für verschiedene Zielgruppen)
- Einbindung verschiedener Stakeholder (Gremien, „early adopter“)
- Anpassung der vorhandenen Prozesse an den Cloud-Dienst (z.B. Support-Strukturen, Beschaffungsprozess, ...)

Einzelne Aspekte dazu sind im Folgenden nochmal ausführlicher dargestellt.

### 4.1.1. Schulungen

Ist die Entscheidung für ein Cloud-Produkt gefallen, muss vor der Einführung der Schulungsaufwand geklärt/geschätzt werden und Schulungen müssen pro Stakeholder mit genügend Vorlauf durchgeführt werden.

- (technische) Schulungen für Administratoren in der IT (zentral oder dezentral), die den Cloud-Dienst verwalten
- Schulungen für die IT-Mitarbeitenden, die Kunden den Cloud-Dienst als Service anbieten/vermarkten (Erwartungen des Kunden und Benefit für den Kunden beachten)
- Schulungen für die Support-Mitarbeitenden im jeweiligen Support-Level (vgl. Kapitel 2.5. zur Cloud-Strategie und 2.6. zu den Rollen/wer macht was)
- Schulungen für strategische Stakeholder, z.B. Gremienmitglieder der Personalräte, um das Know-how dort auszubauen
- Schulungen für die Early Adopter und die Endnutzer (ggf. andere Inhalte und Schulungsformate, je nach Background der User); Early Adopter können auch als Spreader eingesetzt und geschult werden

Es ist gemeinsam mit dem Anbieter des Cloud-Dienstes ein Konzept zu erarbeiten, welche Schulungen intern und welche mit externer Begleitung durchgeführt werden. Es bietet sich z.B. an, dass Stakeholder durch Externe geschult werden und dann wiederum intern einen Teil der Schulungen z.B. für das Support-Personal übernehmen.

#### 4.1.2. Einbindung verschiedener Stakeholder (Gremien, „early adopter“)

Neben der Einbindung der Stakeholder bei der strategischen Entscheidungsfindung, ist es von Vorteil, diese bei der konkreten Umsetzung frühzeitig zu beteiligen.

Darüber hinaus macht es Sinn, verschiedene Gruppen hier zusammenzubringen, z.B. Nutzende in Form der Early Adopter und Gremienvertreter wie z.B. Personalräte. Die Early Adopter sind meist eine Gruppe, die motiviert ist, den neuen Service zu testen und ihre Anforderungen im Vorfeld formuliert. Als erste User und „Spreader“ kann die Einbindung dieser Gruppe der Hochschule organisatorisch wie strategisch weiterhelfen. So können auf der einen Seite Bedarfe besser erkannt und verstanden werden sowie auf der anderen Seite frühzeitig Bedenken geäußert und Lösungen dafür gefunden werden.

### 4.2. Technische Umsetzung

Die Umsetzung der technischen Rahmenbedingungen ist abhängig vom Anbieter. In den Anlagen 5.4. und 5.5. finden sich Beispiele zur Umsetzung bei Microsoft M365 und Azure.

### 4.3. Go Live

Bevor alle potenziellen Nutzenden Zugang zu dem Cloud-Produkt erhalten, empfiehlt es sich, eine Test- oder Pilotphase durchzuführen. In dieser Phase können die zuvor erarbeiteten Prozesse und technischen Lösungen in kleinerem Umfang getestet und ggf. angepasst werden.

#### 4.3.1. Aktive Begleitung durch die Gremien (z.B. Datenschutzbeauftragte/Personalräte)

Die Unterstützung bzw. Akzeptanz der Gremien der Hochschule spielt eine wichtige Rolle für den Erfolg der Einführung. Durch eine Pilot- oder Testphase bietet sich die Möglichkeit, die Gremien aktiv schon im Vorfeld mitzunehmen und darüber hinaus Nutzende (= Pilotkunden) und Gremien, koordiniert durch die zentrale IT, zusammenzubringen. So können den Nutzenden die entstehenden Mehrwerte erläutert und der Aufbau von Know-how und Verständnis gefördert werden.

Aus den so gewonnenen Kenntnissen können entsprechende Dokumente wie Dienstvereinbarungen, Nutzungsbedingungen o.Ä. erstellt werden.

#### 4.3.2. Definition und Durchführung von Kommunikationsmaßnahmen

Die Einführung von Cloud-Diensten sollte wie jede Organisationsentwicklungsmaßnahme von geeigneten Kommunikationsaktivitäten begleitet werden. Der Begriff „Cloud-Dienste“ ist im Allgemeinen stark emotional besetzt. Die einen sehen hier hohe Rationalisierungspotenziale, andere einen Jobkiller und weitere den Verlust der eigenen Datenhoheit. Eine frühzeitige Kommunikation der Ziele und möglicher Folgen sorgt für Transparenz.

Die Kommunikationsmaßnahmen richten sich hierbei nach innen, also an das eigene Unternehmen, aber auch nach außen im Sinne von Public Relation.

Bei der **internen Kommunikation** ist zu unterscheiden zwischen der Informationsvermittlung an notwendig zu beteiligende Gremien und der Informationsvermittlung mit dem Ziel, die Belegschaft mitzunehmen. Beide Zielgruppen müssen frühzeitig eingebunden werden, die Gremien auch aus formalen Gründen. Die Mitarbeitenden müssen ebenfalls frühzeitig beteiligt werden, um Bedrohungsszenarien zu reduzieren und aus „Betroffenen" „Beteiligte" zu machen. Zu empfehlen ist hierbei eine ständige Kommunikation über den gesamten Projektverlauf. Mögliche Kommunikationsmittel können z.B. persönliche Informationen auf Mitarbeiterversammlungen, Printmedien und natürlich diverse elektronische Medien sein.

Die **externe Kommunikation** richtet sich an die interessierte Allgemeinheit. Gerade bei Hochschulen kann von einem hohen und breiten öffentlichen Interesse ausgegangen werden. Sie bewegen sich i.d.R. nicht in einem produktspezifisch definierten Bereich, sondern stehen im allgemeinen öffentlichen Fokus. Eine klare Kommunikationsstrategie nach außen soll dazu dienen, die öffentliche Meinung im Hinblick auf die Cloud-Strategie der Hochschule positiv zu gestalten. Mögliche Maßnahmen können z.B. Pressearbeit sein oder „Tage der offenen Hochschule", aber auch klassische Kommunikationsmittel. Wichtig ist auch hier eine frühe Einbindung der zukünftigen Hochschulklientel und ihrer Bezugspersonen. Während Schülerinnen und Schüler tendenziell eher Cloud-affin sind, kann das bei Lehrenden und Eltern anders aussehen.

## 4.4. Betrieb und Verstetigung

### 4.4.1. Betriebliche Aufwände und Aufgaben

Im Vergleich zu den initialen Aufwänden, die eher ihren Schwerpunkt beim Thema Technik und Kommunikation haben, sind die mittel - bis langfristigen Aufwände vielfältiger:

- Beratung: Potenziell steigt dieser Aufwand mit jedem weiteren Cloud-Anbieter, da anwenderspezifische Details bei der Beratung berücksichtigt werden müssen. Der genaue Aufwand hängt stark von der Aufgabenverteilung innerhalb der Hochschule sowie der Cloud-Strategie ab (Wie viel Beratung leistet die Hochschule? Wann kommen externe Anbieter ins Spiel?).

- Schulungen: Der Bedarf wird stetig sein, sofern die Cloud-Angebote in das normale Portfolio der Hochschule eingehen. Neue Mitarbeitende müssen geschult werden, Änderungen bekannt gemacht werden.

- Support und Dokumentation

- Technik: Hier entfällt meist der Aufwand für Updates, da diese durch den Cloud-Anbieter vorgenommen werden. Die Infrastruktur aufseiten der Hochschule, z.B. zur Bereitstellung der Authentifizierung, muss natürlich weiterhin verwaltet und gewartet werden. Dazu kommt die technische Administration der Software, bei der Änderungen und neue Features im Auge behalten werden müssen.

- ständiger Weiterbildungsbedarf: Die Angebote der Cloud-Anbieter unterliegen meist einer großen Dynamik (siehe z.B. die Apps bei M365 oder der Umfang von AWS). Dienste kommen hinzu, werden in ihren Funktionalitäten geändert oder fallen wieder weg. Hier ist eine ständige Kontrolle erforderlich. Anstehende Änderungen ziehen häufig Schulungsbedarf für Endanwender, aber auch Administratoren nach sich. Diese müssen proaktiv ausgelegt werden. Insbesondere neue Dienste dürfen erst nach sorgfältiger Prüfung der Funktionalitäten, Abhängigkeiten von anderen Diensten und Würdigung der Datenschutzaspekte sowie unter Einbeziehung der zu beteiligenden Gremien aktiviert werden.

### 4.4.2. Auswirkungen auf lokale Systeme und Prozesse

Je nachdem ob Cloud-Angebote als Ergänzung zu bestehenden Services oder als (Teil-)Ablöse gesehen werden, hat dies unterschiedliche Auswirkungen auf die lokalen On-Premise-Systeme. Folgende Aspekte sollten unabhängig davon beachtet werden:

- Verwendung lokaler Systeme als Fallback oder Backup: Die Verstetigung der Cloud-Nutzung erfordert immer auch die Einbeziehung möglicher Exit-Strategien. Dies kann die Rückführung zu lokalen Installationen sein, aber auch die Migration zu anderen Cloud-Anbietern. Die Rückführung zu lokalen Installationen erfordert die Bereithaltung oder zumindest die Möglichkeit zum Aufbau eigener Ressourcen. Eventuell ist es in diesem Zusammenhang auch sinnvoll, lokale Kopien zumindest der geschäftskritischen Daten vorzuhalten.

- Monitoring der Netzwerklast bzw. ggf. notwendiger Ausbau der Netzwerkinfrastruktur: Die Verlagerung von Diensten in die Cloud erhöht die Ansprüche an die Netzwerkinfrastruktur – und zwar sowohl für interne Strukturen als auch für die externe Anbindung der Hochschule. Hier ist über ein Monitoring die Zuverlässigkeit der Verbindung ständig zu prüfen. Gegebenenfalls können Anpassungen der Infrastruktur genauso wie der Außenanbindung erforderlich sein. Hier sind u.a. Aspekte wie Redundanz und Bandbreite in die Überlegungen einzubeziehen. Im Zuge des auch in Hochschulen zunehmenden Einsatzes mobiler Arbeitsplätze ist die Nutzung von Cloud-Diensten Teil des Enterprise Mobility Managements.

- Schnittstellen zwischen „on Premise“ und Cloud: Um eine nahtlose Integration der neuen Services in das vorhandene Portfolio zu ermöglichen und die Akzeptanz der Nutzenden zu erhöhen, sind Schnittstellen ein wichtiger Aspekt. Das gilt nicht nur für hybride Anwendungsszenarien, sondern auch für die Integration von Diensten (On-Premise–Cloud und Cloud–Cloud) ineinander.

- Mobiles Arbeiten: Cloud-Dienste können standortunabhängig genutzt werden und sind damit für die Verwendung beim mobilen Arbeiten wie geschaffen. Der Trend zum mobilen Arbeiten wurde durch Corona noch verstärkt. Das sollte bei zukünftigen Vertragsverhandlungen, z.B. im Bereich des Enterprise Mobility Managements, berücksichtigt werden.

### 4.4.3. Einführung weiterer Cloud-Anbieter

Viele Punkte aus diesem Dokument lassen sich genauso auf die Einführung weiterer Cloud-Anbieter anwenden. So lassen sich z.B. Schemata für die Einführung an der eigenen Hochschule entwickeln, die zu einem beschleunigten Verfahren führen können.

Im Sinne der Multi-Vendor-Strategie ist es sinnvoll, weitere Cloud-Anbieter (auch mit überschneidendem Angebot) in das Portfolio der Hochschule aufzunehmen. Darüber hinaus sollte hier aber auch darauf geachtet werden, dass die Cloud-Angebote nicht nur „nebeneinander“ zur Verfügung stehen,

sondern durch Schnittstellen sowohl ineinander als auch in die On-Premise-Angebote integriert werden (Interoperabilität).

## 4.5. Empfehlungen

### 4.5.1. Empfehlungen für Rechenzentren

- Kommunikation, Kommunikation, Kommunikation
- frühzeitige Einbindung notwendiger Gremien: Personalräte, CIO(-Gremium), Gruppenvertretungen, Datenschutzbeauftragte
- mehrstufiger Einführungsprozess
- Einbindung von „Cloud-willigen“ Einrichtungen als Pilotnutzern
- Aufbau von Cloud-Know-how in den Gremien
- Schaffung einer Austauschplattform mit Pilotkunden, Rechenzentrum, Gremien zur Förderung von Verständnis
- Berücksichtigung der Auswirkungen auf lokale Systeme bei der Nutzung der Cloud
- Berücksichtigung der mittel- bis langfristigen Aufgaben, auch bei der Personalstrategie
- Bezug zur Nachhaltigkeitsstrategie der Hochschule
- Erstellung eines Konzepts zum langfristigen Betrieb

# 5. Anhang

## 5.1. Autoren

Die Autorinnen und Autoren sind allesamt Mitglieder der ZKI-Kommission Cloud. Sie stammen aus verschiedenen, über das gesamte Bundesgebiet verteilten Einrichtungen und verfügen über unterschiedliche Hintergründe, sodass eine sehr breite Expertise zusammengeführt werden konnte.

| Name | Rolle/Einrichtung |
|---|---|
| **Daniel Bündgens** | Leitung der Kommission<br>Geschäftsführer, IT Center, RWTH Aachen University |
| **Denise Dittrich** | Stellv. Leitung der Kommission<br>Gruppenleitung Anwendungsbetrieb und Cloud, IT Center, RWTH Aachen University |
| **Nicole Bargsten** | Teamleitung Softwareadministration, IT.SERVICES, Ruhr-Universität Bochum |
| **Oliver Christ** | Abteilungsleiter IT-Services, Technische Hochschule Mittelhessen |
| **Christian Fötinger** | Stabsstelle Informationssicherheit staatlicher bayerischer Hochschulen und Universitäten |
| **Alexander Giebelhaus** | Stabsstelle Cloud-Architektur und Management, Universität Passau |
| **Oliver Göbel** | Stabsstelle Informationssicherheit, Universität Stuttgart |
| **Simon Graupe** | Leitung der Stabsstelle Datenschutz und behördlicher Datenschutzbeauftragter, Leibniz Universität Hannover |
| **Patrick von der Hagen** | Stellv. Abteilungsleitung Anwendungen, Middleware und IT-Architektur am Steinbuch Center for Computing, Karlsruher Institut für Technologie (KIT) |
| **Olaf Jacobsen** | Leiter Bielefelder IT-Servicezentrum, Universität Bielefeld |
| **Gernot Kirchner** | Stabsstelle Datenschutzbeauftragter/Juristische Angelegenheiten, TU Chemnitz |
| **Nikolaj Kopp** | Gesellschaft für wissenschaftliche Datenverarbeitung Göttingen (GWDG) |
| **Johannes Nehlsen** | Stabsstelle IT-Recht der staatlichen bayerischen Hochschulen und Universitäten |
| **Matthias Rack** | Beauftragter für Informationssicherheit, TU Dresden |
| **Dirk von Suchodoletz** | Leiter Abteilung eScience, Rechenzentrum der Universität Freiburg |
| **Elke Spanke** | Business Relationship Managerin für Kooperative Informationsverarbeitung und -versorgung, Karlsruher Institut für Technologie (KIT) |
| **Jens Syckor** | Datenschutzbeauftragter, TU Dresden |
| **Jakob Tendel** | Cloud Services, DFN-Verein |

## 5.2. Mitglieder der Kommission

Neben den Autorinnen und Autoren dieses Dokuments hat die ZKI-Kommission noch folgende Mitglieder:

| Name | Rolle / Einrichtung |
|---|---|
| **Birgit Alkenings** | ZIM, Heinrich-Heine-Universität Düsseldorf |
| **Kerstin Bein** | Leitung Universitäts-IT, Universität Mannheim |
| **Matthias Bestenlehner** | Hochschule Heilbronn |
| **Lars Brehmer** | Zentrum für Informations- und Mediendienste (ZIM), Universität Duisburg-Essen |
| **Christian Bretting** | Technische Hochschule Nürnberg |
| **Ossamma El Abbadi** | Hochschule Ruhr-West |
| **Oliver Diekamp** | Leitung Dezernat für Informations- und Kommunikationstechnik, Ludwig-Maximilians-Universität München |
| **Thomas Habisch** | Freie Universität Berlin |
| **Erik Hecht** | Software- & Lizenzmanagement, Universität zu Köln |
| **Carsten Hellmich** | Hochschule Hannover |
| **Margitta Höftmann** | Bauhaus-Universität Weimar |
| **Jörg Jakobi** | Director ICT Infrastructure Solution, NTT Germany AG & Co. KG |
| **Detlef Janzon** | Identity-, Access- und Security-Management, Ruhr-Universität Bochum |
| **Rene Joachim** | Leitung Sales Development Deutschland – Public Sector, Bechtle |
| **Alexander Kiontke** | Abteilungsleiter Netze und Kommunikationsdienste, TU Dresden |
| **Lars Kühnel** | Abteilungsleiter Benutzer-Service, Christian-Albrechts-Universität zu Kiel |
| **Lutz-Peter Kurdelski** | Chief Information Security Officer, Duale Hochschule Baden-Württemberg |
| **Jan Leendertse** | Universität Freiburg |
| **Alejandra Lopez Vargas** | CIO/Leiterin ZIM, Universität Duisburg-Essen |
| **Andreas Michels** | Zentrum für Informations- und Mediendienste (ZIM), Universität Duisburg-Essen |
| **Thorsten Michels** | Technische Universität Kaiserslautern |
| **Karl Molter** | Leiter des Rechenzentrums, Hochschule Trier |
| **Mihran Müller-Bickert** | Ruhr-Universität Bochum |
| **Manfred Paul** | Leiter Zentrale IT, Hochschule München |
| **Andreas Petersen** | Projektkoordination Zentrale IT-Systeme, Universität zu Lübeck |
| **Torsten Prill** | CIO, Freie Universität Berlin |

| | |
|---|---|
| **Markus Rebensburg** | Abteilungsleiter Server und Storage, Christian-Albrechts-Universität zu Kiel |
| **Michael Röder** | Cloud Services, DFN-Verein |
| **Kirsten Roschanski** | Philipps-Universität Marburg |
| **Albrecht Rösler** | Funktion IT-Rechtsberatung bei der KOPIT - Kooperationsplattform IT Öffentliche Auftraggeber eG (Wiesbaden) |
| **Maja Ruby** | |
| **Inga Scheler** | Stellv. Leitung Regionales Hochschulrechenzentrum, Technische Universität Kaiserslautern |
| **Frank Schreiterer** | Stellv. Leitung des Rechenzentrums, Universität Bamberg |
| **Janne Schulz** | Universität Mannheim |
| **Christian Schultz** | TU Dortmund |
| **Jürgen Schwibs** | IT-Gruppenleiter, TU Darmstadt |
| **Sven Seefeld** | Teamleiter Microsoft-Server, STiNE-Infrastruktur und Virtualisierung, Regionales Rechenzentrum der Universität Hamburg |
| **Thomas Simon** | Leiter Zentrum für Informationstechnologie und Medienmanagement, Universität Passau |
| **Ralf Skujat** | Teamleiter Basisdienste und Support, komm. Teamleiter Linux, Unix und Computational Services, Universität zu Lübeck |
| **Josef Spangler** | Leiter Abteilung Zentrale Systeme, Universität Regensburg |
| **Thomas Starck** | IT-Beschaffung und Leiter des ZIMT-Service, Europa Universität Flensburg |
| **Tania Stephan** | Head of Community Management, SWITCH |
| **Roger Thomalla** | Leiter Haushalt & Controlling, Friedrich-Alexander-Universität Erlangen |
| **Laura Thompsen** | Procurement & Software Licensing, Goethe Universität Frankfurt am Main |

## 5.3. DFN-Cloud: die Cloud-Rahmenvereinbarung „2020 IaaS+“ von GÉANT aus dem OCRE-Projekt

### 5.3.1. Ausgangspunkt

Die GÉANT Association ist die Dachorganisation der europäischen Forschungsnetze, wie der deutsche DFN-Verein, und hat bereits 2016 zum ersten Mal kommerzielle Public-Cloud-Angebote europaweit ausgeschrieben. Im Jahr 2020 hat GÉANT im Rahmen des Projekts „Open Clouds for Research Environments – OCRE“ ein Folge-Vergabeverfahren geleitet, dessen Ergebnisse seit dem ersten Quartal 2021 für Teilnehmereinrichtungen des DFN über die externen Dienste der DFN-Cloud zur Verfügung stehen. Die Vielfalt der verfügbaren Cloud-Angebote konnte deutlich ausgebaut werden und umfasst nun ein Spektrum europäischer und außereuropäischer Angebote – von Hyperscale-Alleskönnern bis zu Boutique-Spezialisten.

Es handelt sich hier um Dienste zur Unterstützung von „Compute & Storage“-Anwendungen, mit Fokus auf Infrastructure Cloud, also virtuelle Maschinen; äquivalente und ergänzende Platform und Software Cloud Services sind wie im jeweiligen Angebot spezifiziert ebenfalls von der Ausschreibung abgedeckt.

### 5.3.2. Die Rahmenverträge

Die Rahmenverträge bieten allgemein folgende Vorteile für Einrichtungen:[17]

- Ausschreibung erfüllt
- finanzielle/Mehrwertvorteile
- von der Ausschreibung abgedeckte Beschaffung von Beratung/Trainingsleistungen
- Flexibilität bei Rechnungsstellung, Bezahlung auf Rechnung
- Datentransfer über die DFN-Zugänge kostenfrei[18]
- deutsches Vertragsrecht, mit Gerichtsstand Deutschland

### 5.3.3. Die unter 2020 IaaS+ in Deutschland verfügbaren Dienste

Aktuelle Informationen und Beschreibungen zu den Diensten und dem Bezugsweg sind jeweils unter folgender Adresse zu finden:

https://cloud.dfn.de

### 5.3.4. Der Beschaffungsweg für Einrichtungen

Die Rahmenverträge dienen in erster Linie dazu, den Beschaffungsweg zu erleichtern, und richten sich an die zentrale IT-Beschaffung an Einrichtungen. Ihre Hauptleistung besteht darin, die Einrichtungen von der Durchführung eines Beschaffungsverfahrens zu entlasten und die o.g. Mehrwerte zu sichern. Es wurden hier keine weitergehenden Verhandlungen über AGB mit den Anbietern geführt, es sollte also bis auf die genannten Punkte von Marktkonditionen ausgegangen werden. Die Rahmenvereinbarungen bieten aber die Möglichkeit, per Miniwettbewerb nachgebesserte AGB einzuholen und dann zu beschaffen.

Der Beschaffungsvorgang sieht im Wesentlichen folgende Schritte vor:

- Teilnahme an der DFN-Cloud (gültiger DFN-Rahmenvertrag, „Dienstvereinbarung“ DFN-Cloud)

[17] Einzelne Angebote enthalten weitere spezifische Dienste des Anbieters, erlauben z.B. ebenfalls die ausgeschriebene Beschaffung der Lernplattform oder der Collaborations-/Produktivitäts-Suite.

[18] Einige Anbieter gewähren dies unter Vorbehalt einer Verhältnismäßigkeitsklausel.

- ausreichend konkrete Spezifikation des Cloud-Bedarfs (entweder Ressourcenumfang oder Plattformeigenschaften)
- Abgleich mit den verfügbaren Angeboten und Auswahl nach einer von drei Methoden
    - Direktauswahl
    - Selbstständiger Vergleich nach Aktenlage
    - voller Miniwettbewerb
- Dokumentation der Auswahl und Begründung in einem internen Vergabevermerk
- Unterzeichnung der Abrufvereinbarung „Call-off Contract“ mit ausgewählten Anbietern

– bis hier entgeltfrei und ohne Abnahmeverpflichtung –

- bilaterale Beschaffung der Dienste bei einem Anbieter zu den genannten Konditionen

### 5.3.5. Vergaberecht und Angebotsauswahl

Das Vergabeverfahren wurde durch die zentrale Beschaffungsstelle GÉANT als offenes Verfahren nach EU-Vergaberichtlinie 2014/24/EU durchgeführt und vergab Rahmenverträge an alle Angebote, die die Minimalkriterien erfüllen.

Die Beschaffung durch bzw. mithilfe von Dritte(n) ist in Deutschland in § 120 Abs. 4 GWB und § 4 Vergabeverordnung (VgV) geregelt. § 4 VgV dient der Umsetzung der Regelungen von Art. 38 Richtlinie 2014/24/EU zur gelegentlichen gemeinsamen Beschaffung und zur zentralen Beschaffung durch eine zentrale Beschaffungsstelle mit Sitz in einem anderen Mitgliedsstaat.

Da die GÉANT Association in Amsterdam ansässig ist, kam niederländisches Vergaberecht zur Anwendung, das die Richtline national umgesetzt hat. Als finaler Akt der Vergabe trägt die beschaffende Einrichtung die Verantwortung, eine ausreichend objektiv begründete Auswahl des geeignetsten Angebots zu treffen. Dieser Prozess unterliegt unvermeidbar dem Beschaffungsrecht des Vergabeverfahrens, also dem der Niederlande.

Dazu beschreibt das Vergabeverfahren drei Methoden:

1. Direktabruf: wenn nur ein Angebot der Bedarfsbeschreibung entspricht, die fair und nichtdiskriminierend formuliert wurde
2. Selbstständiger Vergleich nach Aktenlage: wenn mehrere Angebote den Bedarf erfüllen. Die Einrichtung kann mit Daten aus dem Vergabeverfahren und aktuellen Preisinformationen einen Vergleich zwischen allen Angeboten aufstellen und das geeignetste dann per Direktabruf auswählen.
3. Miniwettbewerb: wenn kein Angebot den Bedarf erfüllt. Per Miniwettbewerb können nach spezifizierten Kriterien nachgebesserte Angebote eingeholt werden. Auf die Ergebnisse werden dann Verfahren 1./2. angewendet.

Weitere Anleitungen und Tools zur Unterstützung werden jeweils aktuell auf https://cloud.dfn.de vorgehalten.

### 5.3.6. Vertragsunterlagen

| | **Unterlagen** |
|---|---|
| **DFN** | DFN-Rahmenvertrag<br>Dienstvereinbarung „externe Dienste der DFN-Cloud“ |
| **Anbieter** | Call-off Agreement<br>Service Order o.Ä. |
| **Plattformbetreiber** | OIP Enrollment o.Ä. |

## 5.4. Technische Details zu Microsoft M365

### 5.4.1. Nutzerprovisionierung

Ein Azure Active Directory (Azure AD oder AAD) ist die grundlegende Identitäts- und Zugangsverwaltung für Microsoft-Cloud-Dienste, insbesondere für Microsoft 365 (Teams, OneDrive etc., kurz: M365). Ein Azure AD ist grundsätzlich unabhängig von einem lokalen AD, kann aber gekoppelt werden. Dabei ist es ist möglich, mehrere voneinander unabhängige Azure-AD-Mandanten (bei Microsoft: Tenants) einzurichten.

Bei der Einrichtung wird einem solchen Tenant eine Region zugeordnet, was Auswirkungen auf Lizenzumfang und Speicherort der Daten hat. Eine nachträgliche Änderung ist nur unter bestimmten Bedingungen möglich.

Es ist möglich, ein lokales AD mit einem oder mehreren Azure AD Tenants über Microsoft-Werkzeuge (Azure AD Connect, ADFS) zu koppeln. Unterstützte Szenarien werden in der Microsoft-Dokumentation[19] beschrieben.

Ein Azure AD benötigt jedoch grundsätzlich kein On-Premise Active Directory. Eine reine Cloud-Lösung ist denkbar, wenn die Nutzenden keinerlei On-Premise-Dienste nutzen, die ihrerseits ein lokales AD erfordern. Ein Szenario „alle Alumni sollen ein Postfach @alumni.universitaet.de als lebenslang gültige E-Mail-Adresse bekommen, aber sonst keine Dienste nutzen dürfen“ könnte also komplett in einem Mandanten in der Cloud abgebildet werden.

#### Synchronisation bei vorhandenem Active Directory

Die Übertragung/Synchronisation der Attribute eines lokalen AD in ein Azure AD kann über Azure AD Connect[20] erfolgen. Dabei können gezielt Attribute zur Synchronisierung ausgewählt werden.

[19] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies

[20] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/

Notwendige (synchronisierte) Attribute, damit die Services funktionieren[21]:

- Vorname
- Nachname
- UserPrincipalName: Normalerweise ist dies die E-Mail-Adresse, das kann aber bei der Provisionierung auch anders gewählt werden. Hier sind auch pseudonymisierte Accounts nach dem Schema <ID>@Domain möglich.
- location: Das Attribut muss gesetzt werden, da man ansonsten M365 nicht nutzen kann. *Empfehlung:* Das Attribut nicht synchronisieren, sondern nachträglich automatisiert für alle Nutzenden gleichsetzen.
- sourceAnchor/ImmutableID: gemeinsamer Schlüssel zwischen lokalem AD und AAD; typischerweise ObjectGUID

Weitere empfohlene Attribute:

- E-Mail-Adresse: Die E-Mail-Adresse wird für Benachrichtigungen innerhalb von M365 und Azure genutzt. Es ist daher zu empfehlen, diese korrekt zu setzen, damit man hier über z.B. Aktionen/Freigaben/Nachrichten in M365 informiert werden kann.

*Achtung:* Die E-Mail-Adresse sollte immer eindeutig einem Azure AD Account zugeordnet sein, ansonsten kann es z.B. bei Einladungen zu Problemen kommen.

Über Filter ist es möglich, nur Teile des lokalen Active Directory in die Cloud zu synchronisieren. Damit kann z.B. ein Opt-in umgesetzt werden, bei dem sich die Nutzenden eigenständig für die Synchronisation ins Azure AD freischalten.

Die Synchronisation kann zunächst unidirektional vom lokalen AD in das Azure AD erfolgen, in bestimmten Szenarien werden aber auch Elemente von der Cloud in das lokale AD synchronisiert (z.B. Exchange Hybrid).

### Optionen ohne eigenes Active Directory

Ein AAD kann vollständig über PowerShell verwaltet werden. Mitunter nutzen kommerziell verfügbare IdM-Systeme diese Schnittstellen und stellen Beispiele bereit, womit eine Anbindung einfach möglich ist.

Hinsichtlich der Authentifizierung entfallen dadurch jedoch die in 5.4.2. vorgestellten Varianten 1 und 3, die ein eigenes AD benötigen. Um die Speicherung von Passwörtern in der Cloud zu vermeiden, bietet sich hier nur eine Authentifizierung in Variante 2: Shibboleth ohne AAD Connector und ADFS an.

[21] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-sync-attributes-synchronized

### 5.4.2. Authentifizierung

Grundsätzlich ist es möglich, Passwörter in Hash-Form in der Cloud zu speichern, dann erfolgt auch die Authentifizierung direkt in der Cloud. Besser ist die Integration in vorhandene Single-Sign-on-Systeme wie Shibboleth (mit oder ohne ADFS) oder Authentifizierung über Passthrough. Bei einem Ausfall der On-Premise-Dienste ist dann allerdings kein Zugriff auf reine Cloud-Anwendungen möglich.

#### Variante 1: Shibboleth mit ADFS (Active Directory Federation Services)

Voraussetzungen:

- Shibboleth-Infrastruktur in der Hochschule
- lokales Active Directory, dass die oben genannten benötigten Attribute sowie den sAMAccountName enthält; ADFS muss für das Active Directory (AD) installiert sein
- Der sAMAccountName muss auch im Shibboleth Identity Provider (IDP) bekannt sein.

Hinweis: der sAMAccountName kann hier frei gewählt werden. Es ist z.B. möglich, hier eine selbst definierte ID zu nutzen. Da der sAMAccountName auch immer die Domain des Tenants enthält, kann er z.B. dann <ID>@Domain.de sein.

Aufbau der Infrastruktur:

Benötigt wird auf jeden Fall ein lokales Active Directory, das über einen Azure AD Connect mit dem Azure AD synchronisiert wird. Woher die Daten in dem lokalen Active Directory kommen, ist zweitrangig, solange die oben genannten Voraussetzungen erfüllt werden.

Zusätzlich wird ADFS am AD benötigt, da dieser als Service Provider (SP) dann für Shibboleth dient. Neben der Shibboleth-Konfiguration wird dann dort auch eingestellt, welche Attribute zur Identifikation des Nutzenden verwendet werden. Details dazu finden sich in der Anleitung.

Grober Ablauf der Authentifizierung:

- Öffnen der M365- oder Azure-Anwendung
- Eingabe des Benutzernamens: <XYZ>@CloudDomainderHochschule.de
- Weiterleitung an den lokalen Shibboleth Identity Provider (= ADFS des lokalen Active Directory)
- Eingabe der Credentials in der hochschuleigenen Shibboleth-Infrastruktur
- nach erfolgreicher Authentifizierung: Weiterleitung an M365/Azure
- Identifizierung des Nutzenden: als Attribut von Shibboleth wird der sAMAccountName aus dem AAD mitgegeben, darüber wird dann der richtige Nutzende identifiziert

Hinweis: Ein Login ist somit für alle Personen möglich, die einen Shibboleth-Zugang haben. Nutzen kann M365/Azure aber nur derjenige, dessen sAMAccountName auch im AAD vorhanden ist.

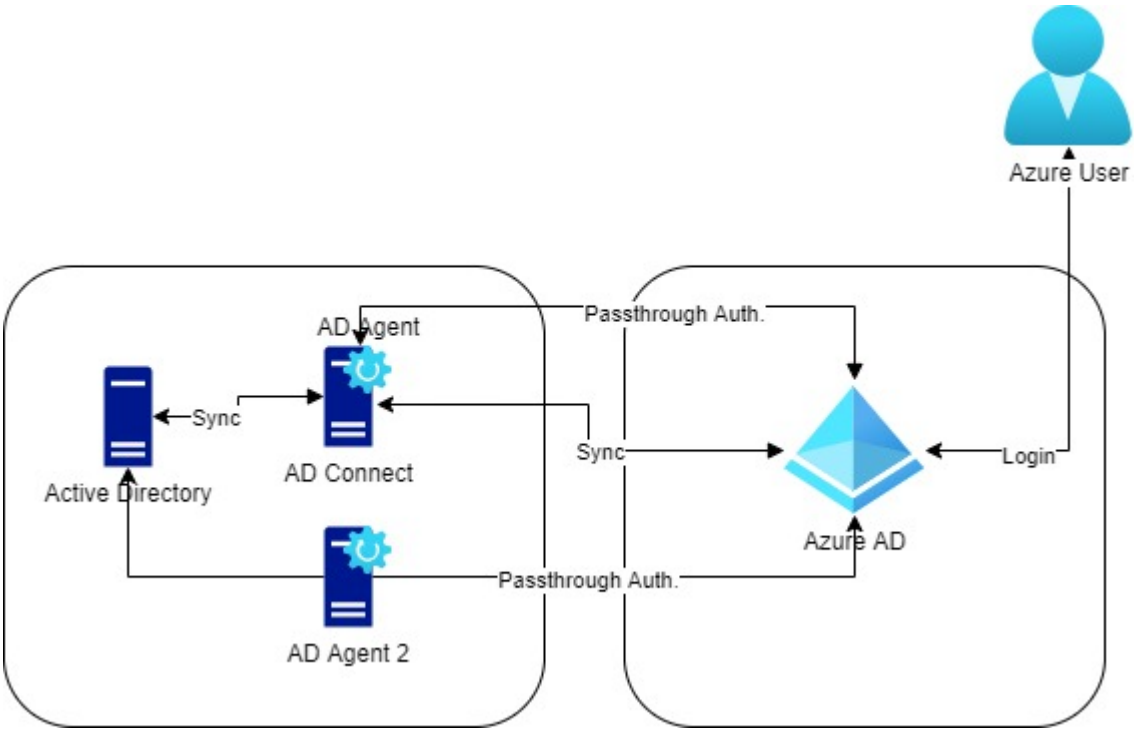
### Variante 2: Shibboleth ohne AAD Connector und ADFS

Microsoft ermöglicht die Koppelung eines Tenants per SAML an einen geeigneten Identity Provider. Dabei kann auch das im Hochschulumfeld verbreitete Shibboleth genutzt werden, auch Keycloak ist im Einsatz. Zu beachten ist leider, dass ein IDP nur einen Tenant bedienen kann, weshalb ggf. Umgehungslösungen gefunden werden müssen. Beispielsweise kann ein Keycloak als transparenter „Proxy“ dienen, der zwischen Tenant und Shibboleth geschaltet wird. Damit werden die Bedingungen von Microsoft erfüllt und die Nutzenden „sehen“ trotzdem ein SSO mit Shibboleth.

Eine detaillierte Dokumentation hierzu wurde vom KIT veröffentlicht.[22]

Die offizielle Dokumentation[23] von Microsoft betont: „Microsoft supports this sign-on experience as the integration of a Microsoft cloud service, such as Microsoft 365, with your properly configured SAML 2.0 profile-based IdP.“ Bei Problemen verweist Microsoft allerdings an den Hersteller-Support des IDP.

### Variante 3: ohne Föderierung: Anbindung des lokalen AD über AD-Connect und Passthrough-Mechanismus




[22] https://blog-about.xyz/2020/03/20/azuread-mit-authentifizierung-am-shibboleth-idp-verwenden/

[23] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-fed-saml-idp

Voraussetzungen:

siehe Dokumentation von Microsoft[24]

Software:

- AD-Connect Tool
- Agent Tool
- (optional) IdFix (für Checkup des lokalen AD)

Microsoft bietet mit dem Azure AD Connector ein Tool an, um das lokale AD mit Azure AD zu verbinden. Dieses Tool wird auf einem eigenen Server installiert.

Das Tool bietet die Möglichkeit, nur einzelne oder alle OUs zu synchronisieren. Weiterhin können auch nur Objekte in bestimmten Gruppen übertragen werden. Dieses Feature soll aber laut Microsoft nicht produktiv genutzt werden und muss bei der Erstinstallation aktiviert werden und aktiv bleiben, sonst verschwindet diese Option. Weiterhin besteht noch die Möglichkeit, anhand von Attributen zu filtern. Damit kann z.B. auch ein Opt-in-Mechanismus abgebildet werden.

Als Authentifizierungsmechanismus nutzen wir Passthrough. Bei dieser Methode wird das Passwort nicht in die Azure Cloud synchronisiert, sondern verbleibt im lokalen AD (im Gegensatz zu Pass-Sync, hier wird das Passwort verschlüsselt übertragen). Dafür müssen lokale Agents installiert werden. Diese übernehmen die Aufgabe, die Authentifizierung gegen das lokale AD durchzuführen. Ein Agent wird bereits bei der Installation von Azure AD Connect mit installiert. Für eine höhere Ausfallsicherheit empfiehlt es sich, noch einen zweiten zu installieren.

Die Auswahl, welche Attribute in die Cloud übertragen werden sollen, kann ebenfalls festgelegt werden. Wir empfehlen aus Datenschutzgründen den Minimalansatz.

Ablauf der Authentifizierung

siehe Dokumentation von Microsoft[25]

### 5.4.3. Administration/Strukturierung

#### Portale

Microsoft stellt diverse Portale zur Verfügung, um die Dienste zu verwalten. Im Folgenden werden die Portale kurz vorgestellt, die am häufigsten zum Einsatz kommen:

- M365 Admin Portal (admin.microsoft.com): allgemeine Einstellungen zum Tenant, den Benutzern und M365-Einstellungen

[24] https://docs.microsoft.com/de-de/azure/active-directory/hybrid/how-to-connect-install-prerequisites

[25] https://docs.microsoft.com/de-de/azure/active-directory/hybrid/how-to-connect-pta

- Portale der einzelnen Anwendungen in M365: spezifische Einstellungsmöglichkeiten zu den Diensten

- Azure Portal: konkretere Einstellungen vor allem zum Thema Benutzerverwaltung, Berechtigungsvergabe und Azure AD Connect

### Initiale Einstellungen

Folgende Einstellungen sollten als Erstes geprüft werden, wenn ein Tenant erstellt oder administrativ übernommen wurde:

- Selbstregistrierung Nutzende: Im Standard können sich Nutzende mit der dem Tenant zugeordneten E-Mail-Domain selbst einen Account im Azure AD erstellen (z.B. vorname.nachname@unidomain.de bei der Domain des Tenants unidomain.onmicrosoft.com).

- Selbstregistrierung Rechner: Bei der Anmeldung eines Nutzenden ist es möglich, auch gleichzeitig den Rechner im Azure AD zu registrieren.

- Welche Lizenzen sind verfügbar und welche Apps können verwendet werden? Hier lassen sich sowohl die einem Nutzenden zugeordneten Lizenzen als auch die in einer Lizenz verfügbaren Apps einschränken.

### Administrative Berechtigungen: Globale Administratoren

Die administrativen Accounts sollen unabhängig von der gewählten Authentifizierung für die Nutzenden funktionieren, um im Notfall reagieren zu können. Das bedeutet in den meisten Fällen, dass zusätzliche Cloud-Accounts für die (wenigen) globalen Administratoren eingerichtet werden sollten – in der Form Nutzername@domain.onmicrosoft.com. Für diese Konten sollte unbedingt die Multi-Faktor-Authentifizierung (MFA) aktiviert werden, entweder per dedizierter Einstellung für den Account[26] oder über eine Richtlinie im „Bedingten Zugriff“[27].

Zudem muss beachtet werden, dass alle Accounts, auch globale Administratoren, im Tenant sichtbar sind (z.B. bei der Berechtigungsvergabe oder der Suche nach Personen in Teams). Um diese Accounts nicht mit den normalen Benutzer-Accounts zu verwechseln, bietet es sich an, dem Namen hier einen Zusatz (z.B. „adm“) hinzuzufügen.

### Administrative Berechtigungen: Zugriffe für den Support

Es ist sinnvoll, den Support-Mitarbeitenden dedizierte Berechtigungen im Tenant zu geben, um z.B. Standardfälle direkt bearbeiten können. Dazu gehört z.B. der Zugriff auf die Daten der Nutzenden im Azure AD. Hierbei sollten die Accounts zum Support von den Accounts zur täglichen Nutzung getrennt werden. Auch in diesen Fällen sollte auf MFA nicht verzichtet werden. Die Differenzierungsmöglichkeiten hinsichtlich der Berechtigungen hängen ggf. vom Azure-AD-Lizenzplan (P1/P2) ab.

---

[26] https://docs.microsoft.com/de-de/azure/active-directory/authentication/howto-mfa-userstates

[27] https://docs.microsoft.com/de-de/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa

Bei mehreren Tenants ist es möglich, die Benutzer aus dem Support in einem Tenant zu pflegen und in die anderen Tenants als Gäste einzupflegen.

### 5.4.4. Tenant-Verwaltung

Grundsätzlich ist es möglich, für eine Hochschule mehrere Tenants zu verwalten, auch durch die Kopplung mit einem lokalen AD und eine passende Filterung beim Einsatz von Azure AD Connect. Da hier noch wenig Erfahrung in der Hochschul-Community besteht, kann hier keine klare Empfehlung ausgesprochen, sondern es können nur Erfahrungswerte weitergegeben werden.

#### Trennung von verschiedenen Benutzergruppen

Es ist möglich, unterschiedliche Benutzergruppen in unterschiedlichen Tenants zu pflegen, z.B. Studierende und Mitarbeitende aufzuteilen. Dabei sind folgende Aspekte zu berücksichtigen:

- Multi-Tenant-Betrieb muss in den Verträgen (z.B. MS-Bundesvertrag, OCRE-Rahmenvertrag) berücksichtigt werden, ist aber grundsätzlich möglich.
- Die Tenants brauchen unterschiedliche Domains. Im Zusammenhang mit Exchange Online oder Exchange Hybrid sind hier ggf. Abhängigkeiten zu beachten, die einen Multi-Tenant-Betrieb kompliziert oder unmöglich machen.[28, 29]
- Um eine Zersplitterung über viele Tenants zu vermeiden, können auch in einem Tenant unterschiedliche „Administrative Units“ definiert werden, um Nutzergruppen zu trennen, z.B. nach Institutszugehörigkeit.[30]
- Der Umgang mit Nutzenden, die zu mehreren Gruppen gehören, muss in jedem Fall beachtet und ein entsprechender Prozess etabliert werden. Hierbei sind z.B. auch Fragen der Lizenzierung (doppelte Lizenz?) zu klären.

#### Gemeinsame Verwaltung von M365 und Azure in einem Tenant

Die Verwaltung von M365 und Azure erfolgt in beiden Fällen über einen Tenant, die Organisation der Nutzenden über das dort integrierte Azure AD. Es stellt sich hier die Frage, ob es daher sinnvoll ist, die Verwaltung über denselben Tenant laufen zu lassen, so wie es Microsoft auch empfiehlt. Im Folgenden sind einige Argumente pro und contra aufgeführt:

[28] https://www.msxfaq.de/cloud/identity/o365multiforestdirsync.htm

[29] https://techcommunity.microsoft.com/t5/exchange-team-blog/september-2020-hybrid-configuration-wizard-update/ba-p/1687698

[30] https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units

Pro:

- Nutzerprovisionierung und -authentifizierung müssen nur einmal implementiert werden.
- Lizenzen der Nutzenden müssen nur einmal beschafft werden (z.B. wenn generell A5 für alle Administrations-Account aufgrund von 2FA genutzt werden soll).

Contra:

- M365 und Azure haben unterschiedliche Nutzergruppen. Zugang zu Azure wird meist nur von einigen wenigen IT-affinen Nutzenden benötigt, M365 dagegen potenziell von allen Nutzenden.
- Je nach Nutzung werden ggf. unterschiedliche Attribute für die Nutzenden benötigt.
- zusätzliche Komplexität im Tenant

### Umgang mit bestehenden, selbst verwalteten und viralen Tenants

Es ist theoretisch möglich, mit jeder vorhandenen E-Mail-Adresse der Hochschule (inkl. Subdomains) ein Microsoft-Konto zu erstellen. Besitzt eine Hochschule nun mehrere Domains, so stellt jede dieser Domains einen potenziell eigenen Tenant dar.

Durch die Nutzung des kostenfreien Microsoft-M365-Angebots für Bildungseinrichtungen[31] ist die Wahrscheinlichkeit, dass es weitere Tenants zu den unterschiedlichen Domains der Hochschule gibt, gestiegen.

In der Regel werden Administratoren der Hochschule die viralen Mandaten im ersten Schritt übernehmen[32]. Anschließend kann ein solcher Mandant z.B. abgekündigt und deaktiviert oder aber als regulärer Mandant über ein IdM-System oder Azure AD Connect in geordnete Pflege- und Verwaltungsprozesse eingebunden werden.

Ein Azure AD Connect würde versuchen, die vorhandenen Konten z.B. anhand der E-Mail-Adressen mit einem lokalen AD zu verknüpfen. Das sollte entsprechend vorbereitet werden.[33]

[31] https://www.microsoft.com/de-de/education/products/office?ms.officeurl=students

[32] https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover

[33] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-existing-tenant

### 5.4.5. Lizenzierung und Abrechnung

#### Abrechnung

Die Abrechnung von M365-Diensten (i.d.R. bezieht sich das auf die gebuchten Lizenzen oder Zusatzprodukte) erfolgt entweder über den entsprechenden Vertragspartner (z.B. über den MS-Bundesvertrag) oder per Kreditkarte.

#### Lizenzierung

Für den Bereich „Education“ gibt es drei verschiedene Lizenzen, die für M365 relevant sind: A1, A3 und A5. Eine Übersicht der dort enthaltenen Features findet sich auf den Seiten von Microsoft[34].

Die wichtigsten Unterschiede zwischen den Lizenzen sind in den Details zu finden, so bieten z.B. A3 oder A5 mehr Möglichkeiten der Verwaltung oder bestimmte Sicherheitsfeatures. Da sich dies aber auch ändern kann, sollte im konkreten Fall immer an Microsoft oder einen Vertragspartner für Fragen herangetreten werden.

Je nach gewünschter Funktion müssen nicht alle Konten über die gleiche Lizenz verfügen, z.B. nur administrative Accounts.

#### Zuweisung von Lizenzen

In einem AAD können gleichzeitig verschiedene Lizenzen verfügbar sein. So kann bspw. für die meisten Konten eine A1-Lizenz ausreichen, während ausgewählte Konten eine A3- oder gar A5-Lizenz benötigen. Über die Attribute und dynamische Gruppen lassen sich Benutzer-Lizenzgruppen zuweisen (also Gruppen, denen eine Lizenz zugeordnet wurde und deren Mitglieder diese Lizenz ebenfalls bekommen). Weiterhin ist es natürlich möglich, die Zuweisung manuell in Azure AD zu erledigen. Auch mit PowerShell kann eine Lösung implementiert werden.

Bei der Zuweisung unterscheidet Microsoft einzelne Lizenzen in unterschiedliche „Lizenzoptionen“. Konkret beinhaltet eine A1-Lizenz u.a. die Optionen „Teams“ und „SharePoint“. Diese können bei der Lizenzzuweisung einzeln aktiviert oder deaktiviert werden, sodass Szenarien wie „an der Hochschule sind die Voraussetzungen für den Einsatz von Teams gegeben, aber nicht für den Einsatz von SharePoint“ an dieser Stelle abgebildet werden können.

### 5.4.6. Netzwerk

#### Allgemeines

Für allgemeine Überlegungen bietet sich die Dokumentation von Microsoft[35] an. In vielen Fällen sind diese Überlegungen/Optimierungen im ersten Schritt jedoch verzichtbar. Je nach geplantem Nut-

[34] https://docs.microsoft.com/de-de/office365/servicedescriptions/office-365-platform-service-description/microsoft-365-education

[35] https://docs.microsoft.com/en-us/microsoft-365/enterprise/networking-roadmap-microsoft-365?view=o365-worldwide

zungsumfang verlagert sich lokaler Verkehr ggf. in die Cloud und belastet damit die Außenanbindung. Das dürfte insbesondere Dienste wie Exchange Online oder auch OneDrive betreffen, die allerdings üblicherweise gute Caching-Mechanismen haben.

#### MS Teams

Als Dienst für Telefonie und/oder Videokonferenzen ist Teams besonders sensibel, z.B. bzgl. Latenzen. Die Dokumentation und Unterstützung seitens Microsoft[36] sollte deshalb vor der Einführung beachtet werden, ein dauerhaftes Monitoring bietet sich an.

#### Überlegungen zu VPN

Insbesondere in Homeoffice-Szenarien, bei denen der Netzwerkverkehr der Mitarbeitenden zunächst per VPN zur Universität geleitet wird, können Probleme entstehen. Der Datenverkehr vom Nutzer zur Uni, von dort in die Cloud und wieder zurück belastet die Außenanbindung mindestens mit doppeltem Volumen.

Im Worst Case nutzen mehrere Mitarbeitende aus dem Homeoffice heraus MS Teams über VPN für eine Besprechung, was sowohl die Außenanbindung der Universität als auch die VPN-Server belastet. Insbesondere ist die Teams-Nutzung besonders sensibel bzgl. Latenzen, sodass die Qualität in diesem Szenario schnell leiden kann.

Es kann sich daher anbieten, alternativ zum klassischen VPN-Zugang auch einen „Split-VPN-Zugang“ anzubieten, über den nicht der gesamte Datenverkehr aus dem Homeoffice über VPN in die Universität läuft. Damit läuft die Teams-Nutzung direkt zwischen den Anwendern und der Microsoft-Cloud, was die Ressourcen der Universität schont und gleichzeitig durch niedrige Latenzen die Qualität für die Nutzer verbessert.

### 5.4.7. Hinweise zu konkreten Apps in M365

Grundsätzlich können sich die Apps, die in M365-Lizenzen enthalten sind, ad hoc ändern. Es ist daher ratsam, diese regelmäßig zu überprüfen, um keine unbeabsichtigte Nutzung zu ermöglichen.

#### Standort

Verschiedene Apps können anderen DSGVO-Bedingungen unterliegen als der Tenant selbst. So werden bspw. Sway und Planner nicht unbedingt auch am Standort des Tenants gehostet[37].

#### Kollaboration

Apps zur Kollaboration, wie z.B. Teams, sind nur sinnvoll nutzbar, wenn man den Kommunikationspartner auch klar identifizieren kann. Dafür ist es notwendig, den Klarnamen im Azure AD zu führen und nicht nur rein anonymisierte Nutzende. Darüber hinaus kann es bei einer großen Anzahl an Nutzenden hilfreich sein, zusätzliche Merkmale (wie z.B. die E-Mail-Adresse) sichtbar zu machen.

---

[36] https://docs.microsoft.com/en-us/microsoftteams/prepare-network

[37] Stand April 2021

#### Zusätzliche Apps in Teams

Innerhalb von Teams können zwei verschiedene Arten von Apps zusätzlich integriert werden: Microsoft-Apps (z.B. Planner) oder Apps von Drittanbietern. Hier ist die Empfehlung, alle Apps erstmal zu sperren, dann gezielt zu prüfen und einzeln wieder nach Bedarf freizugeben.

## 5.5. Technische Details zu MS Azure

Die Nutzung der IaaS- bzw. PaaS-Ressourcen erfolgt in einem Tenant. Dabei kann es sich um einen Tenant handeln, der auch für die SaaS-Dienste M365 verwendet wird, sodass keine eigene Konfiguration hinsichtlich Nutzerprovisionierung oder Authentifizierung erforderlich ist.

Ein besonderes Augenmerk ist auf die Strukturierung des Tenants zu legen, bei der die „Subscriptions“ genutzt werden können. Über diese können Ressourcen aus administrativen Gründen oder auch für die Abrechnung gebündelt werden.

Ein weiteres Augenmerk sollte auf die Kostenkontrolle gelegt werden. Durch die nutzungsbezogene Abrechnung kann eine vergessene virtuelle Maschine schnell zu hohen Kosten führen, die je nach Abrechnungsmodell unerwartet belastet werden oder ein vorher definiertes Budget aufbrauchen, was zum Ausfall der Dienste führen kann.

### 5.5.1. Nutzerprovisionierung

siehe 5.4.1.

Zusätzlich ist hier zu beachten, dass je nach Berechtigungsmodell zusätzliche Attribute, wie z.B. die Zugehörigkeit zu einem Projekt oder einer Einrichtung mit provisioniert werden sollten.

### 5.5.2. Authentifizierung

siehe 5.4.2.

### 5.5.3. Administration/Strukturierung

#### Subscriptions/Abonnements

Innerhalb von Azure werden Ressourcen in verschiedenen Hierarchien verwaltet:

- Ressourcen sind in Ressourcengruppen organisiert.
- Ressourcengruppen sind Subscriptions/Abonnements zugeordnet.

Subscriptions sind also die Möglichkeit, die Ressourcen innerhalb eines Tenants zu organisieren. Diese können z.B. zur Trennung von einzelnen Projekten oder Einrichtungen verwendet werden.

Für die Vergabe von Berechtigungen stellen Subscriptions eine eigene Ebene dar. Das bedeutet, dass gezielt Berechtigungen auf konkrete Subscriptions vergeben werden können.[38]

Darüber hinaus hat jede Subscription eine eigene Übersicht über die dort generierten Kosten. Subscriptions können also gezielt als Abrechnungsebene eingesetzt werden.

### EA-Portal/Zuordnung von Verträgen zu Subscriptions

Das Portal Microsoft Azure Enterprise (ea.azure.com) bietet eine Übersicht über die der Hochschule (bzw. dem eingeloggten Account) zugeordneten Verträge[39].

Achtung: Initial hat hier nur der Account Zugriff, der zu der im Vertrag genannten E-Mail-Adresse gehört.

Folgende Aspekte sind im EA-Portal zu beachten:

- Nutzung der vorgegebenen Strukturen: Im Standard ist im EA-Portal eine Struktur mit Departments und diesen zugeordneten Accounts vorgesehen. Diese Struktur kann genutzt werden, um seine Organisationsstruktur in Azure abzubilden. Es wird mittlerweile aber von Microsoft eher empfohlen, dafür Management Groups zu verwenden.[40] Es muss mindestens ein Department und ein Account angegeben werden, um dem Vertrag zugeordnete Subscriptions anlegen zu können.

- Anlegen von Subscriptions: Zum Anlegen von Subscriptions (egal ob automatisiert, über das EA- oder über das Azure-Portal), die unter einem bestimmten Vertrag laufen sollen, muss immer einer der im EA-Portal unter einem Department angegebenen Accounts genutzt werden. Andernfalls findet keine korrekte Zuordnung statt.

- Single oder Multi-Tenant: Um Accounts in verschiedenen Tenants zu nutzen und darüber dann auch Subscriptions in verschiedenen Tenants anzulegen, muss das „Auth level“ auf „Work or School Account Cross Tenant“ gesetzt werden. Achtung: Das ist z.B. schon notwendig, wenn der initiale Account (z.B. vorname.nachname@hochschule.de) zu einer anderen Domain gehört als der für Azure genutzte Tenant (z.B. azure.hochschule.de).

[38] https://docs.microsoft.com/de-de/azure/role-based-access-control/rbac-and-directory-admin-roles#azure-roles

[39] https://docs.microsoft.com/de-de/azure/cost-management-billing/manage/ea-portal-administration

[40] https://docs.microsoft.com/de-de/azure/governance/management-groups/overview

#### Schnittstellen

Innerhalb von Azure gibt es diverse Schnittstellen, u.a.:

- Schnittstellen zur Automatisierung von Abläufen innerhalb von Azure (Automation), z.B. über PowerShell
- API zur Verwaltung des Tenants, z.B. Ansprechen des Azure ADs, Anlegen von Subscriptions
- Einbindung von externen Services über den Azure Marketplace

#### Grundsätzliche Einstellungen: Umsetzung von Richtlinien

Sofern hochschulweite Richtlinien zur Nutzung von Azure verhandelt wurden, sollten diese, soweit möglich, auch technisch umgesetzt werden. Dafür können z.B. Blaupausen genutzt werden. Sinnvolle Richtlinien könnten z.B. sein:

- Beschränkung der nutzbaren Regionen für Ressourcen (z.B. auf Deutschland oder Europa)
- Beschränkung der nutzbaren Dienste in Azure
- verpflichtende Nutzung von bestimmten Tags (z.B. Kostenstelle, Ansprechpartner, …)
- Namenskonventionen
- Beschränkung der nutzbaren Ressourcen (z.B. für eine Blaupause „Linux Praktika“ nur die günstigsten Linux-VMs)
- verpflichtende Anzahl an Ownern für eine Subscription

Die Richtlinien können dabei sowohl für Ressourcen als auch für Ressourcengruppen und Subscriptions gelten.

Die Blaupausen werden auf Subscriptions angewendet, entweder beim Erstellen oder nachträglich.

Achtung: Die Fehlermeldungen, wenn z.B. eine Ressource aufgrund von Richtlinien nicht erstellt werden kann, sind nicht sehr aussagekräftig und lassen keine direkten Rückschlüsse auf die Blaupause zu!

### 5.5.4. Abrechnung und Lizenzierung

#### Abrechnung

Im Standard wird für Azure eine Rechnung von Microsoft pro Tenant generiert und diese vom Vertragspartner an die Hochschule weitergegeben. Möchte man eine andere Ebene der Abrechnung, so muss dies mit dem Vertragspartner vereinbart werden.

### Bezahlart

- Monetary Commitment: Diese Art der Bezahlung kann wie ein Prepaid-Guthaben verstanden werden. Im Vorfeld wird eine konkrete Summe beim Vertragspartner bestellt und in Rechnung gestellt. Diese Summe wird dann auf den Vertrag der Hochschule gebucht und kann zur Nutzung in Azure verwendet werden.

  *Achtung:* Das Guthaben ist zeitlich immer an die Vertragslaufzeit gebunden, d.h., zum Ende der Vertragslaufzeit verfällt das Guthaben!

  *Achtung:* Das Guthaben ist an einen Vertrag gebunden, nicht an einen Tenant oder eine konkrete Subscription!

- Pay as you go: Hier erhält die Hochschule monatlich (bzw. nach festgelegtem Datum) eine Rechnung über die bis dato genutzten Ressourcen.

### Kostenübersicht

Die aktuellen Kosten für Azure können in (mindestens) zwei verschiedenen Portalen eingesehen werden:

- Enterprise Portal ea.azure.com: Zugang hierzu haben nur die Personen, die extra für die Einsicht in die Verträge berechtigt sind (weitere Zugänge können eingerichtet werden). Hier sind die gesammelten Kosten aufgeführt, die dem laufenden Vertrag zugeordnet sind. Diese können auch auf mehreren Tenants entstanden sein.

- Azure Portal portal.azure.com: Hier ist eine Kostenübersicht sowohl über den gesamten Tenant als auch über einzelne Subscriptions oder ressourcengenau möglich.

Achtung: Die Ansicht der generierten Kosten ist nicht stundenaktuell, sondern ca. 24–48 Stunden alt. Nutzt man einen Vertrag in mehreren Tenants, ist eine Gesamtübersicht nur im Enterprise Portal möglich.

### Lizenzierung

Hier muss man zwischen zwei Lizenzen unterscheiden:

- Lizenzen, die für den Zugang zu Azure und die Benutzerverwaltung relevant sind: Es gibt spezielle Features im Azure AD, die eine entsprechende Lizenz des Nutzenden voraussetzen, z.B. eine Lizenz Azure AD Premium P1 oder P2.

- Lizenzen zur Nutzung von Ressourcen in Azure: Generell benötigen Ressourcen in Azure wie auch „on premise“ eine Lizenz, je nachdem welche Software/Middleware hier verwendet wird. Diese Lizenzkosten fallen also zusätzlich zu den Kosten für die Ressourcen an. Bei einigen Anbietern gibt es allerdings spezielle Konditionen zur Nutzung von Cloud-Ressourcen wie z.B. Azure Hybrid Benefit.[41]

[41] https://azure.microsoft.com/de-de/pricing/hybrid-benefit/