Cloud Management

Änderungen in Verwaltungs- und Bereitstellungsprozessen

Zentren für
Kommunikation und
Informationsverarbeitung e.V.

Inhalt

Autoren

Autor:innen der ZKI-Kommission Cloud:
Denise Dittrich (Sprecherin), Elke Spanke (stellv. Sprecherin)
Birgit Alkenings, Nicole Bargsten, Dirk Bei der Kellen, Bernd Beining, Ingrid Bohr, Angela Ebert, Nadine Fritz, Christian Fötinger, Jacqueline Gerland, Patrick von der Hagen, Michael Heckel, Gernot Kirchner, Nikolaj Kopp, Christian Meyer, Thorsten Michels, Christian Schultz, Thomas Schuster, Julia Seidel, Christian M. Stracke, Dirk von Suchodoletz, Gina Weiland

ZKI e.V. unterstützt durch den Vorstand
Torsten Prill – Freie Universität Berlin

1.Einleitung

Die ZKI-Kommission Cloud wurde 2019 gegründet und hatte das Ziel, einen Leitfaden für alle ZKI-Mitgliedshochschulen zu erstellen, der die Einführung von Cloud-Leistungen an Hochschulen beschreibt. Der Leitfaden (ZKI, 2021) wurde im Jahr 2021 veröffentlicht. Eine weitere Publikation zu Themen der digitalen Souveränität im Bildungsbereich (ZKI, 2022) folgte im November 2022. Aufgrund der anhaltenden Nachfrage nach weiteren Ergebnissen und Empfehlungen wurde die Kommission unter der Leitung von Denise Dittrich (stellv. Abteilungsleiterin Systeme und Betrieb, IT Center, RWTH Aachen University) und Elke Spanke (Business Relationship Managerin, Stabsstelle Digital Office, Karlsruher Institut für Technologie [KIT]) verlängert bis März 2024. Der Auftrag für die Fortsetzung der Kommission war, einen weiteren Leitfaden zu erstellen, dessen Fokus auf den Prozessänderungen, vor allem in Beschaffung und Betrieb von Cloud-Leistungen, liegt.

1.1. Differenzierung zu den bisherigen Ergebnissen der Kommission

Der Schwerpunkt des ersten Ergebnisberichts der ZKI-Kommission Cloud lag auf dem Prozess der Einführung von neuen Cloud-Leistungen, inklusive der Betrachtung von anhängigen Themen wie Datenschutz und Informationssicherheit oder auch Cloud-Strategien. Alle dort getroffenen Aussagen bilden die Grundlage für dieses Dokument.

Vorhandene Entscheidungsprozesse und -strukturen sind die Grundlage dafür, dass die Hochschulen adäquat agieren können. In der vorangegangenen Publikation der ZKI-Kommission Cloud (ZKI, 2022) wurde auf diese Grundlagen eingegangen und es wurden Forderungen formuliert, um bessere Rahmenbedingungen zu schaffen. Diese Forderungen sind hinsichtlich ihrer Relevanz und der Diskussion rund um die digitale Souveränität und Nachhaltigkeit weiterhin aktuell und gültig.

Wie auch der erste Ergebnisbericht bezieht sich das vorliegende Dokument auf Aufgaben und Prozesse an deutschen Hochschulen. Durch die weiter fortgeschrittene Verbreitung und Nutzung von Cloud-Leistungen an Hochschulen ist aktuell der Bedarf hoch, insbesondere die Prozesse zu betrachten, die im dauerhaften Umgang mit Cloud-Leistungen relevant sind.

1.2. Motivation und Ziele

Mit der verstärkten Durchsetzung von Cloud-basierten Betriebs- und Dienstbereitstellungsmodellen ändert sich eine Reihe von Rahmenbedingungen. Wahrscheinlich wird es zukünftig kaum noch Hochschulen geben, die nur lokale Installationen auf Endbenutzersystemen oder Servern im ausschließlichen Einflussbereich der jeweiligen Einrichtung nutzen (können). Auch noch verfügbare lokal installierte Software integriert zunehmend einzelne Cloud-Funktionen, bspw. die Lizenzverwaltung über „Named Licenses“ in Portalen der Hersteller oder den Zugriff auf KI-Funktionen realisiert durch Backends in der Cloud.

Technische Innovationen finden mehr und mehr nur noch in der Cloud statt und zunehmend werden Cloud-Leistungen zu Gütern, die überhaupt erst die Grundlage für eine funktionierende Forschungs- und Ausbildungslandschaft schaffen. Letzteres wird insbesondere dann verstärkt, wenn vonseiten der Hersteller Cloud-Leistungen – im Unterschied zu lokal installierbaren Produkten – vorrangig aktualisiert und gewartet werden.

Aus Sicht der Anbieter schafft der Umstieg auf ein Cloud-Modell einige Vorteile, z.B. muss kein Support für eine Vielzahl möglicher On-Premises-Umgebungen geleistet werden, es muss keine Vielzahl von Versionen unterstützt werden und durch regelmäßige Zahlungen entstehen kontinuierliche Einnahmen über den

gesamten Nutzungszeitraum. Gleichzeitig bewerben die Cloud-Anbieter Argumente wie z.B. das zentrale Patch- und Sicherheitsmanagement oder generell den ausgelagerten Betrieb, die als Mehrwerte höhere Preise rechtfertigen sollen. Es ist also davon auszugehen, dass Cloud-Modelle dauerhaft durch die Hersteller forciert werden und eine Rückkehr zu On-Premises-Angeboten nicht zu erwarten ist.

Aus ökonomischer Sicht der Hochschule sind Cloud-Leistungen in erster Linie klassische Miet- bzw. Leasing-Angebote, die zwar auf Dauer kalkulierbare Kosten zu sein scheinen, aufgrund ihrer Bezahlmodalitäten aber häufig mit aktuellen (Beschaffungs-)Prozessen in Hochschulen kollidieren. Nötig ist deshalb ein Kulturwandel in der Beschaffung, bei der Erstellung von Verträgen und dem Software-Lizenzmanagement, im Betrieb der IT-Infrastrukturen sowie bei den Nutzenden der Leistungen. Daher sind die Prozesse von der Bedarfsermittlung über die Genehmigung bis zur Beschaffung zu überarbeiten. Ebenso müssen die Behandlung von Verträgen und das Lizenzmanagement in oben genannten Bereichen neu konzipiert werden. Eine kooperativere Zusammenarbeit zwischen Strategie-, IT- und Fachebene wird erforderlich sein.

1.3. Aufbau des Dokuments

Die Gliederung des hier vorliegenden Dokuments orientiert sich an den Prozessen, beginnend bei der Steuerung von Anfragen seitens der Nutzenden nach einer Leistung, die eine Cloud-Leistung darstellt oder Cloud-Leistungen beinhaltet, über die Prozesse im Management von Beschaffungen bis hin zu Bereitstellung und Betrieb von Cloud-Leistungen. Sofern nicht anders definiert, gelten alle Aussagen für alle Cloud-Servicemodelle (siehe 5.3).

Zielgruppe des Dokuments sind Entscheidungsträger:innen in den Hochschulen, z.B. Hochschulleitungen wie Kanzler:innen und Präsidien, CIOs sowie RZ-Leitungen, die die angesprochenen Änderungen gemäß Governance in die Hochschule tragen müssen und verantworten.

In den einzelnen Kapiteln werden grundsätzliche, anbieterneutrale Feststellungen getroffen und dann anhand von kurzen, spezifischen Beispielen (optisch abgehoben in blauen Boxen) erläutert oder konkretisiert. Ausführlichere Beispiele zu Diensten des Deutschen Forschungsnetzes (DFN) finden sich im Anhang.

Des Weiteren sind im Anhang die Autor:innen des Dokuments sowie alle weiteren Mitglieder der ZKI-Kommission Cloud zu finden.

1.4. Begriffsklärungen

In diesem Dokument werden einheitliche Begriffe verwendet, die synonym für eine ganze Gruppe stehen:

- Cloud-Leistungen als Überbegriff für Cloud-Lösungen und -Dienstleistungen sowie für alle Services und Bereitstellungsmodelle

- Cloud-Anbieter als Überbegriff für Hersteller, Vendor, Hyperscaler, Anbieter föderaler Leistungen

Darüber hinaus wird neben den Service- und Bereitstellungsmodellen (siehe 5.3) auch der Grad der Cloud-Nutzung bei Leistungen unterschieden. Die Bandbreite reicht hier von der reinen Cloud-basierten Vergabe des Nutzungsrechts für eine lokal installierte Software bis hin zur Speicherung und Verarbeitung von (weiteren) Daten in der Cloud.

Innerhalb des Spektrums unterscheiden sich die Fälle hinsichtlich der damit verbundenen Risiken und Abhängigkeiten und damit in den Prozessen der Bereitstellung und des Betriebs.

Weitere Begriffsklärungen finden sich in Kapitel 5.2.

2. Strategische Überlegungen

Neben den im 1. Ergebnisbericht (ZKI, 2021) bereits ausführlich dargelegten Aspekten für strategische Entscheidungen sind mittlerweile weitere Punkte in den Fokus der Betrachtung gerückt. Auch sie sollten Teil der Cloud-Strategie einer Hochschule sein.

2.1. Ergänzung zu den bisherigen Rahmenbedingungen

Wie bereits erläutert, ist die Cloud-Strategie einer Hochschule mit entsprechenden Leitplanken Basis für eine strukturierte Cloud-Nutzung. Um die Prozesse schlank zu halten, müssen ein klares Rollenverständnis definiert und die Entscheidungsträger ausdrücklich benannt sein. Grundsätzlich sollten bei einer Cloud-Nutzung immer eine Prüfung und eine Freigabe im Rahmen der von der Hochschulleitung verabschiedeten Cloud-Strategie erfolgen.

2.1.1. Mitbestimmung

Die Einführung und die Nutzung von Cloud-Leistungen unterliegen ähnlich wie lokale Datenverarbeitungen nach den landesgesetzlichen Regelungen in vielen Fällen der Mitbestimmung durch die Personalvertretung. Dies begründet sich in der Tatsache, dass technische Verfahren eingeführt und angewandt werden sollen, die objektiv dazu geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen. Weitere Mitbestimmungstatbestände können sich u.a. aus Änderungen in Arbeitsmethoden oder -abläufen ergeben. Ein gelungenes Mitbestimmungsverfahren setzt dabei in jedem Falle voraus, dass mit einer angemessenen Vorlaufzeit und damit rechtzeitig vor der Einführung der beabsichtigten Maßnahme das Vorhaben mit der Personalvertretung erörtert und alle hierfür erforderlichen Informationen umfassend von Seiten der Hochschule zur Verfügung gestellt werden.

Aufgrund der Komplexität von Cloud-Leistungen kann es insbesondere auch erforderlich werden, der Personalvertretung geeignete personelle und technische Ressourcen zur Verfügung zu stellen, um die Tragweite des Einsatzes der Cloud-Leistung nachzuvollziehen und prüfen zu können. Vor diesem Hintergrund und um einer Informationsasymmetrie entgegenzuwirken, bietet es sich insbesondere an, Vertreter der Personalvertretung bereits im Rahmen von Anbieterpräsentationen oder technischen Einführungsveranstaltungen zu beteiligen.

Im Ergebnis des Mitbestimmungsverfahrens kann der Abschluss von Dienstvereinbarungen stehen. Hierfür ist vor der geplanten Einführung oder Nutzung einer Cloud-Leistung hinreichend Zeit einzuplanen.

2.1.2. Datenschutz

Hilfestellung zur Einhaltung der von der Datenschutzgrundverordnung (DSGVO) geforderten Gewährleistungsziele bietet insbesondere das sogenannte Standard-Datenschutzmodell in der aktuellen Version 3.0 (SDM, 2022), das von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 24. November 2022 verabschiedet wurde und damit in allen Bundesländern von den Behörden als Nachweis der datenschutzrechtlichen Rechenschafts- und Nachweispflicht anerkannt wird. Auch im Zusammenhang mit der Einführung und Nutzung von Cloud-Leistungen erlaubt das SDM eine strukturierte Überprüfung und Einhaltung der datenschutzrechtlichen Gewährleistungsziele und ist deshalb geeignet, als Teil der Cloud-Strategie einer Hochschule datenschutzrechtlich Prüfungen zu begleiten und zu monitoren. Die Anwendung des SDM ist zudem im „IT-Grundschutz-Kompendium“ des BSI vorgesehen (Bundesamt für Sicherheit in der Informationstechnik, 2023, Abschnitt CON2 „Datenschutz“.

Der Hochschule obliegt es nunmehr, bei der Einführung und Nutzung von Cloud-Leistungen auf der Infrastrukturebene den gesamten Lebenszyklus der zu verarbeitenden personenbezogenen Daten abzubilden und mit geeigneten technischen und organisatorischen Schutzmaßnahmen hinsichtlich der Gewährleistungsziele und damit ausgehend vom Schutzbedarf der Daten (Datenklassifizierung) zu definieren und zu überprüfen. In der Praxis haben sich zur Umsetzung der SDM-Anforderungen Checklisten oder Fragenkataloge bewährt, die es den Anbietern bereits in der Vergabephase ermöglichen, gezielt Maßnahmen für die jeweiligen Prozessschritte zu benennen, die erforderlich sind, damit die infrage stehende Cloud-Leistung für die geplante Verarbeitung der personenbezogenen Daten datenschutz- oder allgemein klassifizierter Daten regelkonform eingesetzt werden kann.

2.2. Gestiegene Verantwortung bei den Nutzenden

Durch die Nutzung von Cloud-Leistungen steigt die Verantwortung für den korrekten Umgang mit Daten und Leistungen bei den Entscheidenden und Nutzenden.

Bis vor einiger Zeit war die auf einem Arbeitsplatz zur Verfügung stehende Software fest definiert, durch die zentrale und/oder dezentrale IT-Administration kontrolliert und meist On-Premises betrieben. Datenhaltung und Speicherung lagen lokal in der Hochschule und die Reichweite der Kollaboration war meist auf die eigene Einrichtung beschränkt. Das damit einhergehende Risiko war kalkulierbar.

Durch die einrichtungsübergreifenden Kollaborationen sowie die universelle Verfügbarkeit von Hard- und Software on demand verändert sich das durch die Handlung der Nutzenden entstehende Risiko enorm. Die Details der Cloud-Nutzung sind für die Nutzenden nicht mehr transparent, es sei denn, sie sind ausdrücklich Bestandteil der Vertragsvereinbarungen.

Eine weitere Frage, die sich bei der Auswahl von Cloud-Leistungen stellt, ist, welches Angebot für welchen Anwendungsfall genutzt werden darf. Neben funktionellen Erwägungen sind bei Cloud-Leistungen vor allem der Schutzbedarf der vorliegenden und in der Cloud zu verarbeitenden Daten sowie die rechtlichen Rahmenbedingungen der Cloud-Leistung (z.B. Speicherort, Standort/Herkunftsland des Cloud-Anbieters, vorhandene Verträge) relevant.

Die Nutzenden müssen in die Lage versetzt werden, auch eigenverantwortlich die Vorteile und Risiken der verschiedenen Cloud-Leistungen sowie deren mögliche Einsatzgebiete zu verstehen. Die unterschiedlichen Nutzergruppen aus Wissenschaft und Verwaltung müssen souverän in ihren Tätigkeitsbereichen agieren können.

Dabei können folgende Maßnahmen die Nutzenden unterstützen:

- Awareness-Maßnahmen als Schulungen (z.B. Datenschutz, Informationssicherheit, Cloud-Basics)
- Einbeziehung von Multiplikatoren (z.B. dezentrale IT)
- Handreichungen und Checklisten, z.B. zur Prüfung, welche (personenbezogenen) Daten in welcher Form (bspw. Verschlüsselung, Pseudonymisierung) und bei welchen Cloud-Leistungen (bspw. Datenspeicherung in einem Drittland, Datenspeicherung in der BRD durch ein US-amerikanisches Tochterunternehmen) verarbeitet werden dürfen
- Überblick über sämtliche schon geprüfte Cloud-Leistungen der Hochschule und erlaubte Nutzungsszenarien bzw. Informationsklassen
- Überblick über zur Verfügung stehende Leistungen der Hochschule (als Alternativen zur Cloud-Leistung)
- klare, gut formulierte Nutzungsbedingungen, die die Regeln innerhalb der Hochschule widerspiegeln
- gute Dokumentation und transparente Information zur Datenverarbeitung (ggf. bereitgestellt durch den Cloud-Anbieter)

- Hilfestellung bei der Klassifizierung von Daten; Richtlinie zur Klassifizierung von Daten
- zentrale Beratung, z.B. durch eine zentrale Ansprechstelle (siehe 3.5), Datenschutz- oder Informationssicherheitsbeauftragte

Unbewusste Cloud-Nutzung außerhalb des festgelegten Rahmens
Auch außerhalb kontrollierter Arbeitsumgebungen werden Daten in Cloud-Leistungen verarbeitet, bspw. wenn Personalakten über Teams-Chats geteilt werden oder Google Drive für die Bearbeitung von Forschungsanträgen verwendet wird.

2.3. Datenhoheit der Hochschule

Die Hoheit über die Daten zu behalten ist eng verwoben mit dem Ziel, digital souverän zu agieren. Datenhoheit muss aber nicht zwingend gleichbedeutend mit einer rein lokal auf die Hochschule beschränkten Datenhaltung sein. Vielmehr geht es darum, als Hochschule die Kontrolle zu behalten, z.B. durch die Realisierung von Exit-Strategien oder eine geeignete Back-up-Strategie (siehe 4.1.1). Um die Datenhoheit zu behalten/erhalten, ist Transparenz in unterschiedlichen Dimensionen notwendig. Folgende Maßnahmen sind dabei hilfreich:

- **Sensibilisierung:** Der erste Schritt ist in jedem Fall, Transparenz zu schaffen, wo Daten abgespeichert werden. Dies bedingt eine Sensibilisierung der Nutzenden (siehe 2.2), weil eine technische Erzwingung der korrekten Speicherung nicht in allen Fällen möglich ist.
- **Transparenz über Angebote:** Damit die Nutzenden die korrekte Wahl für die Verarbeitung oder Ablage ihrer Daten treffen können, muss Transparenz darüber existieren, welche Angebote zur Verarbeitung und Speicherung von Daten es überhaupt an der Hochschule gibt. Idealerweise sind diese zentral dokumentiert, zusammen mit eventuellen Einschränkungen bzgl. der Nutzergruppen, Daten oder Speicherorte. Bei diesen Angeboten sollten Datenschutz und Informationssicherheit im Sinne der Hochschule geregelt sein, um größtmögliche Sicherheit zu schaffen.
- **Hochschulweite Richtlinien:** Neben den Angeboten in der Hochschule sollte es Richtlinien geben, die beschreiben, wo welche Arten von Daten verarbeitet und gespeichert werden dürfen. Das kann sich z.B. auf Forschungs- oder Personaldaten beziehen. Eine solche Transparenz schafft Sicherheit bei den Nutzenden und in der Konsequenz hoffentlich eine sicherere Nutzung der externen Dienste.
- **Technische Rahmenbedingungen:** Einige Cloud-Leistungen erlauben Konfigurationen, die z.B. einen Abfluss von Daten außerhalb der eigenen Organisation verhindern. Diese Einstellungen sollten geprüft und entsprechend vorgenommen werden. Eine Interaktion zwischen Cloud-Leistung und dem Identity Management der Hochschule erlaubt weitergehende Einstellungen, wie z.B. einen automatischen Lifecycle (siehe 4.5).
- **Datenformate:** Der Export eines Herstellers ist nur so gut wie der Import des Konkurrenten. Ein Export der Daten einer Whiteboard-Anwendung in Form eines PDF-Dokuments würde zwar weiterhin die erstellten Dokumente verfügbar machen, ohne aber eine weitere Bearbeitung zu ermöglichen. Die Bewertung von Cloud-Leistungen und -Anbietern sollte daher auch darauf basieren, wie sie die Datenportabilität unterstützen. Derartige Anforderungen sollte man in Form einer Checkliste vor der Beschaffung prüfen.

2.4. Hochschulübergreifende Kooperation

Kooperationen können die Hochschulen in bessere Verhandlungspositionen gegenüber den Cloud-Anbietern bringen. Gegenseitige Angebote im Sinne einer Community Cloud reduzieren Abhängigkeiten von Dritten und tragen zur Erhöhung der digitalen Souveränität der Hochschulen bei.

2.4.1. Kooperation auf organisatorischer Ebene

Hochschulen stehen zunächst allein vor der Herausforderung, die Einführung, Nutzung oder Bereitstellung von Cloud-Leistungen zu bewältigen. Nicht nur für kleinere Hochschulen stellt dies regelmäßig eine kaum zu bewältigende Aufgabe dar, auch größere Einrichtungen geraten zunehmend an die Grenzen ihrer Möglichkeiten, wenn die Nutzung von Cloud-Leistungen großer Anbieter abschließend und umfassend bewertet oder der Nachweis des datenschutzkonformen Einsatzes erbracht werden muss.

Kooperationen können auf mehreren Wegen entstehen:

- **Gemeinsame Beschaffungen:** Eine gemeinsame Stimme mehrerer Hochschulen gegenüber den Cloud-Anbietern befördert Erfolge bei Verhandlungen, um Konditionen von bestimmten als gemeinsam notwendig erachteten technisch-organisatorischen Maßnahmen (TOM) bis hin zu Lizenzpreisen für die Hochschulen adäquat gestalten zu können.
- **Teilen von Wissen:** Eine Plattform, über die aktuelle Themen und Herausforderungen rund um den Einsatz der Cloud in der Hochschule ausgetauscht werden können, ist ein wichtiger erster Baustein mit

dem mittelfristigen Ziel eines regelmäßigen Austauschs in einer Arbeitsgemeinschaft der Informierten und Interessierten.

- **Kompetenz-Bündelung:** Die organisatorische Bündelung der Kompetenzen ist eine weitergehende Form der Kooperation. Bei wenigen teilnehmenden Hochschulen macht eine virtuelle Einrichtung wie oben beschrieben Sinn, die lediglich dem Austausch von Wissen dient. Wenn die Anzahl der teilnehmenden Hochschulen steigt, kann eine Bündelung der Kompetenzen in einer gemeinsamen Einrichtung – und damit die Verteilung auf wenige Köpfe –, die allen Hochschulen zur Verfügung steht, höhere Synergie erzeugen und ggf. Komplexität reduzieren.

In der Realität gelingen diese Kooperationen sowohl auf Länder- als auch auf Bundesebene.

ZKI-AK Softwarelizenzen
Auf Bundes- und/oder Länderebene werden viele Softwareverträge seit Jahren gemeinsam verhandelt und vergeben. Beteiligt sind dabei u.a. der ZKI-Arbeitskreis Softwarelizenzen, z.B. bei den Vertragsverhandlungen zum Microsoft-Bundesvertrag oder den Verträgen mit Adobe. Gemeinsame Ausschreibungen sind guter Usus, zumal sie auf Freiwilligkeit der jeweiligen Hochschule beruhen, z.B. bei Adobe, Antiviren-Lösungen, Oracle, SPSS.

Verein zur Förderung eines Deutschen Forschungsnetzes e.V. (DFN)
Seit 2015 beteiligt sich das DFN an der Bereitstellung gewerblicher Cloud-Dienste. Dies geschieht auf europäischer Ebene gesteuert von GÉANT. Aktuell vertritt das DFN die bundesweiten Interessen in Bezug auf kommerzielle Clouds im Ausschreibungsprozess Open Clouds for Research Environments (OCRE).

HITS IT-Beschaffung Bayern
In Bayern wird die Vergabe von relevanten gemeinsamen IT-Bedarfen der bayerischen Hochschulen durch das hochschulübergreifende IT Servicecenter (HITS) Beschaffung koordiniert und organisiert. Das Portfolio des HITS IT-Beschaffung umfasst dabei Hardware, Software und Services - vornehmlich aus dem Bereich der Arbeitsplatzbedarfe und Rechenzentrumsinfrastruktur. Um den Beschaffungsprozess möglichst effizient zu gestalten, wurden durch das HITS IT-Beschaffung möglichst generalisierte Prozesse und Standards definiert, die einzuhalten sind. Dazu gehören bspw. das Benennen von konkreten Ansprechpersonen in jeder teilnehmenden Einrichtung, um den Informationsfluss sicherzustellen, aber auch der allgemeinere fachliche Austausch innerhalb der Rechenzentren, mit Handelspartnern und mit Herstellern.

2.4.2. Kooperation durch Community-Cloud-Leistungen

Neben der Kooperation auf organisatorischer Ebene sind Cloud-Leistungen im Bereich der Community Cloud (siehe 5.3) verfügbar, die entweder von Hochschulen oder z.B. durch das DFN für Hochschulen erbracht werden.

Diese Community-Cloud-Leistungen werden politisch stark gefordert (Wissenschaftsrat, 2023) und vereinen auch aus Hochschulsicht die Vorteile von Cloud-Leistungen mit attraktiven rechtlichen Rahmenbedingungen.

bwCloud
Die bwCloud ist ein föderierter IaaS-Landesdienst für die baden-württembergischen Hochschulen. Auf Basis von OpenStack können virtuelle Maschinen von Mitgliedern der Lehr- und Forschungseinrichtungen des Landes selbst eingerichtet und in Betrieb genommen werden. Betrieben wird die bwCloud an den Standorten Mannheim, Freiburg, Karlsruhe und Ulm. Im Rahmen einer Fortentwicklung (bwCloud 3) sollen weitere Dienste ergänzt werden.

Verein zur Förderung eines Deutschen Forschungsnetzes e.V. (DFN)
Innerhalb der Kategorie der vom DFN-Verein organisierten Dienste gibt es im Rahmen der föderierten Cloud-Leistungen (oder Community Clouds) Angebote wissenschaftlicher Einrichtungen, die über Forschungspartnerschaften zustande kommen, und kommerzielle Angebote gewerblicher Anbieter (externe Cloud-Dienste), die über Vergabeverfahren von Rahmenverträgen organisiert werden.
Eine Kernaufgabe für den DFN-Verein ist die Begleitung der Einrichtungen und die Vermittlung der entsprechenden Leistungen.

Das DFN bietet DFN-eigene Dienste an, diese werden auf DFN-Servern On-Premises betrieben und vom DFN-Verein administriert (z.B. DFNconf, DFN-Terminplaner) oder auch durch beauftragte Dienstleister erbracht (z.B. DFNFernsprechen). Hier liegt ein besonderes Augenmerk auf den Anforderungen an Datenhoheit über den gesamten Datenlebenszyklus, vom Erstellen bis zum Löschen.

Weiterhin bietet das DFN seit geraumer Zeit föderierte Dienste mit Cloud-Anbietern des öffentlichen Sektors an. Aus Sicht des DFN sind dies Community Clouds nach dem Motto „von am Wissenschaftsnetz teilnehmenden Einrichtungen für teilnehmende Einrichtungen“.

3.Changes – Änderungen in Verwaltungsprozessen

Die umfangreichsten Changes in den Verwaltungsprozessen im Kontext von Cloud-Leistungen betreffen das Management von Beschaffungen, das Vertrags- und Lizenzmanagement sowie Änderungen in Informations- und Kommunikationswegen. Die Hochschulen werden auch in den mit Beschaffungen einhergehenden Prozessen einen Kulturwandel zu meistern haben. Es bedarf eines abgestimmten Zusammenwirkens von Strategie, Compliance, Verwaltung sowie zentralem und dezentralem Betrieb der IT-Infrastruktur.

3.1. Beschaffung von Cloud-Leistungen

Cloud-Leistungen erfordern eine andere Art der Betrachtung in Verträgen, Vertragsverhandlungen und in den hochschulinternen Prozessen der Beschaffung als klassische (On-Premises-)Leistungen. Aspekte wie die Verlässlichkeit des Vertragspartners sowie Formen der Abrechnung und Planungssicherheit stellen sich bei Cloud-Leistungen anders dar und müssen geeignet adressiert werden. Die Komplexität von Beschaffungen steigt für alle am Prozess Beteiligten. Strategische Vereinbarungen innerhalb der Hochschule spielen eine bedeutendere und übergeordnete Rolle und müssen Eingang in die Prozessabläufe finden. Exit-Vereinbarungen sind idealerweise bereits im Beschaffungsprozess zu betrachten und einzufordern.

Die gängige Praxis, Beschaffungen von Softwareprodukten und -leistungen unterhalb bestimmter Wertgrenzen dezentral auszulösen, erschwert oder verhindert, dass Strategie- und Compliance-konforme Prozesse gewährleistet werden können. Hinzu kommt die Entwicklung weg von Kauf- hin zu Abo-Modellen, die mit monatlich geringeren Kosten wahrscheinlich unter ebendiese Grenze fallen. Das führt zu einer unvollständigen Übersicht über die vorhandenen Cloud-Leistungen. Daher ist es sinnvoll, Lösungen für möglichst vollständige Übersichten über die vorhandenen Softwareprodukte und -leistungen zu erarbeiten – mindestens auf freiwilliger Mitwirkungsbasis der dezentral IT-Verantwortlichen.

Aus Sicht der Cloud-Anbieter ist die gesamte Hochschule der Abnehmer der Leistung, nicht z.B. ein einzelnes Institut oder ein einzelner Lehrstuhl. Bei Cloud-Leistungen führt das auf mehreren Ebenen zu Herausforderungen:

- Der Cloud-Anbieter hat 100% Transparenz über die Verwendung der bereitgestellten Leistungen, z.B. Lizenzen oder Infrastruktur. Bei fehlender zentraler Verwaltung der Cloud-Leistung durch die Hochschule fehlt diese Transparenz vor Ort und damit ist die Vertragsgestaltung nicht optimierbar.

- Für die Verwaltung von Cloud-Leistungen stellt der Anbieter meist einen Mandanten pro Hochschule bereit. Die Anbindung an zentrale Prozesse, wie z.B. Single Sign-on (SSO), oder die Nutzung von Domains ohne zentrale Bereitstellung ist hier entsprechend komplex. Eine dezentrale Beschaffung bzw. ein dezentraler Betrieb ist somit meist nicht machbar.

- Die Nutzung von zusätzlichen, dezentral genutzten Lizenzen aus zentralen Verträgen (z.B. im Kontext von M365 oder Zoom) muss über zentrale Beschaffungswege erfolgen und entsprechend intern weiter verwaltet und ggf. verrechnet werden.

Es ist hier also regelmäßig zu prüfen, ob eine zentrale Verwaltung von bestimmten Cloud-Leistungen sinnvoll ist, wenn mehrere dezentrale Einheiten diese nutzen (wollen). Checklisten für die Nutzenden oder Beschaffer können hier hilfreich sein sowie Transparenz und Verständnis erhöhen.

3.1.1. Beschaffungsprozess

Nachdem der Bedarf an einer Cloud-Leistung erfasst wurde, beginnt der eigentliche Beschaffungsprozess. In diesem sind mehrere Schritte zu berücksichtigen.

Der Prozess beginnt mit einer Markterkundung. Diese muss, unabhängig davon, ob es sich um eine produktneutrale oder produktspezifische Beschaffung handelt, durchgeführt und dokumentiert werden. Die Markterkundung muss, unabhängig von den Wertgrenzen, so umfassend sein, dass eine fundierte Auswahl eines Produktes stattfinden kann. Hierzu gehören die zu beschaffenden Produkte/ Leistungen, die Eigenschaften des Produktes (Funktionsumfang, Verfügbarkeit [Service Level Agreements, SLAs]), die Eigenschaften des Auftragnehmers, die Erfüllung von Datenschutz und Informationssicherheit, die Vertragsbedingungen, das Lizenzmodell (Nutzungsrechte, Abrechnungsmodell), die langfristigen Gesamtkosten und die Exit-Strategie.

Im Falle einer Ausschreibung für IaaS und/oder PaaS (Infrastructure as a Service, Platform as a Service) gibt es viele standardisierte Produkte, die von verschiedenen Cloud-Anbietern angeboten werden. Damit gibt es echten Wettbewerb, wodurch Bedenken hinsichtlich der digitalen Souveränität entgegengewirkt werden kann. Es sollte daher ein Alarmsignal sein, wenn für ein Projekt mit IaaS/PaaS nur wenige oder gar nur ein einziger Anbieter in Betracht kommen. Wenn bspw. spezifische KI-Funktionen Alleinstellungsmerkmale einzelner Hersteller sind, stellt dies besondere Risiken dar. Das ist dann im Beschaffungsprozess kritisch zu hinterfragen.

In der Regel wird auch berücksichtigt werden, ob ein lokaler Betrieb möglich und ggf. günstiger ist als die Buchung einer Cloud-Leistung. Tendenziell werden interne Betriebskosten eher zu niedrig angesetzt, indem z.B. die Mitnutzung der vorhandenen unterbrechungsfreien Stromversorgung (USV) oder die Back-up-Infrastruktur nicht aufgeführt werden. Hier ist eine Kalkulation im Sinne einer Total Cost of Ownership (TCO) notwendig, um Vergleichbarkeit zu erzeugen. Interne Basiskalkulationen wie „Kosten pro virtuelle Maschine (VM) und Monat“ können unabhängig von einem konkreten Projekt als Referenz erstellt und regelmäßig aktualisiert werden.

Zudem können bei Cloud-Angeboten die Grenzen zwischen den Herstellern von Produkten verschwimmen, da integrierte Drittanbieter-Produkte in Cloud-Leistungen enthalten sein können. Auch mögliche Migrationskosten (z.B. von einer On-Premises-Lösung auf eine Cloud-Lösung) sind zu berücksichtigen.

Ist das Feld der für den Bedarf infrage kommenden Lösungen abgesteckt, muss eine erste Schätzung des Auftragswertes stattfinden und die Wertgrenze ermittelt werden, in der die Beschaffung erfolgt.

Eine besondere Herausforderung im Zusammenhang mit der Cloud ergibt sich dabei vor allem bei der Verwendung von verbrauchsabhängiger Abrechnung („Pay as you go"-Modellen), die es erschweren, die tatsächlichen Bedarfe einzuschätzen und die Nutzenden in ihrem Verbrauch zu beschränken. Es besteht die Gefahr, dass die Wertgrenzen falsch antizipiert werden.

Abhängig vom geschätzten Bedarf wird eine Vergabeart ausgewählt.

Bei der Vertragsgestaltung muss auf die besonderen Eigenschaften von Cloud-Leistungen geachtet werden. Standardmäßig sollten die EVB-IT Cloud Vertragsvorlagen benutzt und individuell angepasst werden.

3.1.2. Nutzung von kostenfreien Angeboten (Beschaffung ohne Beschaffungsvorgang)

Cloud-Anbieter stellen häufig eine (zunächst) kostenfreie Version ihrer Leistung zur Verfügung, die z.B. in ihrem Funktionsumfang, dem Verwendungszweck oder der Verwendungsdauer eingeschränkt ist. Die Nutzung dieser kostenfreien Angebote ohne die Durchführung eines geregelten Beschaffungsvorgangs mit integrierter u.a. rechtlicher Prüfung des Angebotes stellt die heterogene Hochschullandschaft vor besondere Herausforderungen. So werden bspw. Apps, Plug-ins oder Testangebote von Cloud-Leistungen genutzt, ohne dass im Voraus eine Abstimmung oder eine Prüfung stattgefunden hat. Betroffen sind in der Hochschulpraxis insbesondere Cloud-Leistungen wie Umfragetools, Projektmanagementsoftware oder auch Kollaborationstools.

Im Rahmen der zu implementierenden Cloud-Strategie sollten möglichst umfassend alle Cloud-Leistungen betrachtet und deren Einführung und Nutzung abgebildet werden, sodass auch als kostenfrei beworbene Angebote davon erfasst sind. Es sollte ein Prozess implementiert werden, der sicherstellt, dass die Nutzung derartiger Angebote nicht ohne vorherige Freigabe und Prüfung erfolgt. Andernfalls besteht die Gefahr, dass nicht nur Lizenz- und Nutzungsbedingungen nicht hinreichend beachtet werden, sondern zugleich auch Daten der Hochschule und dienstliche Informationen in der Cloud – aufgrund der persönlichen Anmeldungen und Account-Erstellung durch den Nutzenden – nicht mehr zugänglich sind und abfließen.

Aus datenschutzrechtlicher Sicht gilt dies vor allem auch vor dem Hintergrund, dass die vermeintliche Kostenfreiheit z.T. auch damit erkauft wird, dass (personenbezogene) Daten vom Anbieter zu eigenen Zwecken weiterverarbeitet werden. Zu nennen sind bspw. Large Language Models, die als kostenfreie Version für jedermann zur Verfügung stehen, zugleich aber die Kostenfreiheit im Unterschied zur kostenpflichtigen Anwendung dadurch erkauft wird, dass bspw. sämtliche Eingaben auch zu Trainingszwecken weiterverarbeitet werden (dürfen). Ähnliches ist z.B. bei Anbietern von Online-Umfragen der Fall, die personenbezogene Daten für eigene Zwecke verarbeiten und oftmals keine vertragliche Grundlage (z.B. Data Processing Agreement (DPA)) dafür anbieten.

Von Anbietern werden z.T. auch kostenfreie Hochschullizenzen zur eigenen Installation an der Hochschule zur Verfügung gestellt. Auch beim Bezug derartiger Angebote sollte in der Hochschule auf Prozessebene sichergestellt sein, dass der exklusive und in der Regel einmalige Lizenzbezug und die Softwareinstallation nicht ohne Prüfung und vorherige Freigabe im Namen der Hochschulleitung erfolgen. Vordefinierte monetäre Schwellenwerte im Beschaffungsprozess allein sind hierfür nicht mehr hinreichend, sodass zusätzliche Kriterien zu definieren und geeignete Awareness-Maßnahmen (bspw. Checklisten, Schulungen) zu implementieren, ebenso aber auch zielführende Alternativangebote zu schaffen sind.

3.2. Vertragsmanagement

Das Vertragsmanagement ist zwar ein Teil der Beschaffung, es ergeben sich hier aber auch dauerhafte Aufgaben darüber hinaus, vor allem im Kontext von Cloud-Leistungen.

3.2.1. Organisatorische Grundlagen

Voraussetzungen für ein erfolgreiches Vertragsmanagement sind Auffindbarkeit und Vollständigkeit. Konkret bedeutet das:

- Es braucht zentrale Prozesse: Eine Stelle sollte alle Verträge (Software und Hardware) verwalten und abgleichen, ob bereits Leistungen von diesem Hersteller bezogen werden oder diesen entsprechend neu anlegen.

- Diese Verträge sollten zentral abgelegt sein (z.B. im Dokumentenmanagement).

- Geprüft werden sollten, ob vorhandene Verträge der Hochschule für die Nutzenden veröffentlicht werden können. Dies ergibt nicht nur bei Rahmenverträgen Sinn, sondern auch bzgl. der Bündelung

von Lizenzen, Mengenrabatten, Datensicherungen oder der Nachnutzung von bereits erfolgten Abstimmungen. Hier können auch entsprechende Abstufungen gewählt werden, z.B. das gesamte Vertragswerk für den Einkauf, bestimmte Unterlagen für die Nutzenden oder weitere Hochschulen.

- Abgebildet werden sollten (möglichst automatisierte) Lifecycle Workflows, um früh auf Exit-Szenarien reagieren zu können.

Diese Transparenz und das zentrale Management erlauben es, auf rechtliche Änderungen (z.B. EuGH-Urteil zum EU-US Privacy Shield – Schrems II) angemessen zu reagieren, indem die vorhandenen Verträge bekannt und auf bestimmte Merkmale (hier: US-amerikanischer Anbieter) hin geprüft werden können. Daran können dann über Schnittstellen weitere Prozesse angeschlossen werden, um z.B. Informationen oder die Beteiligung von Gremien sicherzustellen.

In jedem Fall ist eine enge Abstimmung zwischen Vertrags- und Lizenzmanagement notwendig, z.B. damit die vorhandenen Lizenzen zu den Verträgen (idealerweise im gleichen Tool) miterfasst werden.

Sinnvollerweise gibt es zudem für übergeordnete Verträge, z.B. auf Landes- oder Bundesebene, entsprechende Datenbanken, in denen gemeinsame Verträge eingesehen werden können.

3.2.2. Cloud-spezifische Prüfpunkte in Verträgen

Auf Basis der oben beschriebenen Daten können dann sowohl bei initialer Beschaffung als auch dauerhaft Prüfungen zu unterschiedlichen Aspekten vorgenommen werden.

Hierbei muss immer die Erforderlichkeit der Leistung im Vordergrund stehen, um Aufwand und Nutzen entsprechend in der Waage zu halten.

Folgende Cloud-spezifische Aspekte sind insbesondere relevant:

- Auswirkungen auf Rechtsgrundlagen der Nutzung (z.B. Verwendungszweck)
- Einschränkungen bei den Nutzergruppen innerhalb der Hochschule und Nutzung durch Externe
- vorhandener Auftragsverarbeitungsvertrag (AVV bzw. Data Processing Agreement, DPA)
- Abrechnungsmodalitäten, z.B. Rechnung oder Kreditkarte, „Pay as you go" oder Vorkasse
- EVB-IT Cloud als individuell anpassbare Vertragsvorlage
- Prüfung der Exit-Bedingungen, z.B. Nachnutzung nach Ende der Vertragslaufzeit, Übergangsfristen zur Datensicherung, Kündigungsfristen innerhalb der Vertragslaufzeit
- Service Level Agreements (SLAs): Neben Verfügbarkeitszeiten ist auch zu regeln, was bei Ausfällen seitens des Cloud-Anbieters passiert, z.B. bei einem Hackerangriff oder Hardwareausfall. Hier sind Aspekte wie z.B. Rechte der Hochschule oder die Haftung des Cloud-Anbieters zu klären. Diese müssen mit vorhandenen Notfallstrategien innerhalb der Hochschule abgeglichen werden.
- Festlegung der Informationspflicht der Cloud-Anbieter gegenüber der Hochschule, z.B. bei Ausfällen oder Sicherheitsproblemen

3.2.3. Vertragsrelevante Änderungen durch den Cloud-Anbieter

Updates seitens des Cloud-Anbieters können Auswirkungen auf bestehende Verträge haben. Das betrifft in technischem Sinne z.B. den Funktionsumfang, aber auch Aspekte wie den erlaubten Verwendungszweck sowie die Nutzung von personenbezogenen Daten durch den Cloud-Anbieter zu eigenen Zwecken.

Unsere Empfehlung ist daher, anstehende Updates und deren Auswirkungen auf bestehende Regelungen und Verträge regelmäßig zu prüfen. Bei steigender Anzahl an Cloud-Leistungen können diese Prüfungen beliebig umfangreich werden. Hier können kollaborative Ansätze helfen, den Gesamtaufwand zu verringern, in dem z.B. pro Bundesland oder deutschlandweit Expert:innen für bestimmte Cloud-Leistungen identifiziert und mit der Prüfung beauftragt werden.

Spätestens bei Vertragsverlängerungen, besser bei jeder Anpassung, sollten die mit dem Vertrag zusammenhängenden Dokumente, wie z.B. DPA, Transfer Impact Assessment (TIA), geprüft werden. In der Hochschule sollte dafür ein Prozess festgelegt werden, damit klar ist, wer die Prüfung anstößt und wer zu beteiligen ist (z.B. Vertragsmanager, DSB, Personalvertretungen, IT).

Neben organisatorischen Aspekten gibt es auch bei technischen Updates und Änderungen entsprechende Prüfpunkte (siehe 4.3).

Microsoft M365
Änderungen im Funktionsumfang der M365-Apps können Auswirkungen z.B. auf Vereinbarungen mit der Personalvertretung, den Umfang der bereitgestellten Apps oder die Verarbeitung von Daten für weitere Zwecke haben. Jedes neue DPA muss hinsichtlich Datenschutzkonformität geprüft werden. Ein aktuelles Beispiel ist hier die Integration von Bing Chat Enterprise in die A3- und A5-Lizenzen.

3.2.4. Vertragsmanagement und Community-Cloud-Produkte

Bei der Nutzung von Community-Cloud-Angeboten gibt es grundsätzliche eine andere Vertragssituation als bei Public-Cloud-Anbietern. Daher sind hier andere Aspekte bei der Nutzung zu beachten:

- Vertragsgrundlage/Prüfung, auf Basis welcher Verträge die Cloud-Leistung verwendet wird: Gibt es einen bestehenden Kooperationsvertrag oder einen Rahmenvertrag, z.B. in einem bestimmten Projekt, das als Basis genutzt werden kann? Oder kann eine individuell angepasste Version der EVB-IT Cloud Rahmenverträge, die intern zur Verfügung gestellt wird, genutzt werden?
- hochschulübergreifende Verrechnung
- Auftragsverarbeitungsvertrag (DPA)
- SLAs: Aktuell sind SLAs mit klaren Aussagen zu Verfügbarkeits- oder Supportzeiten eher unüblich. Aspekte wie der Umgang mit Ausfällen müssen hier ebenso geregelt werden.

In der Rolle als Dienstleister von Community-Cloud-Leistungen im Hochschulkontext gibt es darüber hinaus auch noch weitere Aspekte:

- Prüfung der Skalierbarkeit: Muss mit jeder nutzenden Hochschule ein eigener Vertrag abgeschlossen werden oder ist z.B. eine Art Rahmenvertrag für ein Bundesland möglich?
- Einbeziehung von Fördermittelgebern

3.3. Informations- und Kommunikationswege

Eine gezielte und strategische Nutzung von Cloud-Leistungen kann nur gelingen, wenn erforderliche Informationen für die Nutzenden verfügbar sind und transparente Kommunikationswege u.a. für Beratungsangebote zur Verfügung stehen. Nutzende sollten nicht vor die Herausforderung gestellt werden, Informationen eigenständig und außerhalb der Hochschulverantwortung beschaffen zu müssen, um die Funktionsweise und Eigenschaften einer von der Hochschule bereits geprüften Cloud-Leistung nachvollziehen zu können.

Die Hochschulen müssen die Beschäftigten und Studierenden mittels geeigneter Angebote zur Stärkung der Daten- und Medienkompetenzen (Digital Literacy) in die Lage versetzen, Cloud-Leistungen souverän einzusetzen und zu bewerten.

Hochschulübergreifende Kooperationen, bspw. übergreifende Koordinierungsstellen oder Kompetenzzentren, können hilfreich unterstützen und weitere Expert:innen zur Verfügung zu stellen.

3.4. Lizenzmanagement

Angesichts der wachsenden Anzahl von Softwareprodukten und der stark steigenden Softwarekosten ist eine zentrale und gezielte Verwaltung dringend geboten. Das Lizenzmanagement sollte entlang der Empfehlungen aus Kapitel 2 und 3 dieses Dokuments austariert werden und fester Bestandteil der Beschaffungsprozesse sein. Richtlinien und Prozesse für ein zentrales (und dezentrales) Lizenzmanagement durch oder mit einer zentralen Koordinationsstelle können u.a. sein:

- zentrales Lizenzmanagement (gezielter Lifecycle von Anfrage über Beschaffung und Betrieb bis hin zu Stilllegung/Entzug)
- Schnittstellen zum Einkauf und Betrieb der Cloud-Leistungen
- stetige Lizenzoptimierung in Kooperation mit Nutzenden und Hochschulleitung

Lizenzmanagement umfasst damit organisatorische, buchhalterische und technische Aspekte, die gemäß der Governance der Hochschule in entsprechenden Prozessen gelebt werden sollten.

Empfehlung: Das Lizenzmanagement sollte bereits vor der Beschaffung eingebunden werden, um Empfehlungen für eine optimale Lizenzierung und die passende technische Anbindung geben zu können. Zudem kann zu Alternativprodukten beraten werden.

Entlang der zentral festgelegten Prozesse muss im Lizenzmanagement außerdem geklärt sein, welche Daten in der Cloud gespeichert sind oder sein dürfen (z.B. nur Account-Daten oder auch weitere Daten) und was mit diesen passiert, wenn die Lizenz entzogen wird oder ausläuft (siehe 4.1.2). Dies ist wichtig, weil die Daten oftmals an der persönlichen Lizenz hängen und beim Löschen des Accounts in der Regel ohne Back-up unwiederbringlich gelöscht sind. Bei zentraler Lizenzierung bieten die Cloud-Anbieter z.T. allerdings schon einen Unternehmensspeicher statt eines Speichers auf Nutzerebene an.

Eine Zusammenarbeit zwischen zentralem (organisatorischem) und technischem Lizenzmanagement ist erforderlich.

Dabei muss genau abgewogen werden, ob die Hochschule mit solchen Lösungen umgehen kann. Ohne effiziente interne Prozesse kann der Verwaltungsoverhead potenzielle Einsparungen negieren.

Aus den weiter oben genannten Gründen ist ein Lizenzmanagement auch notwendig, wenn für die Lizenzen keine Kosten anfallen (siehe 3.1.2).

3.4.1. Organisatorisch & buchhalterisch

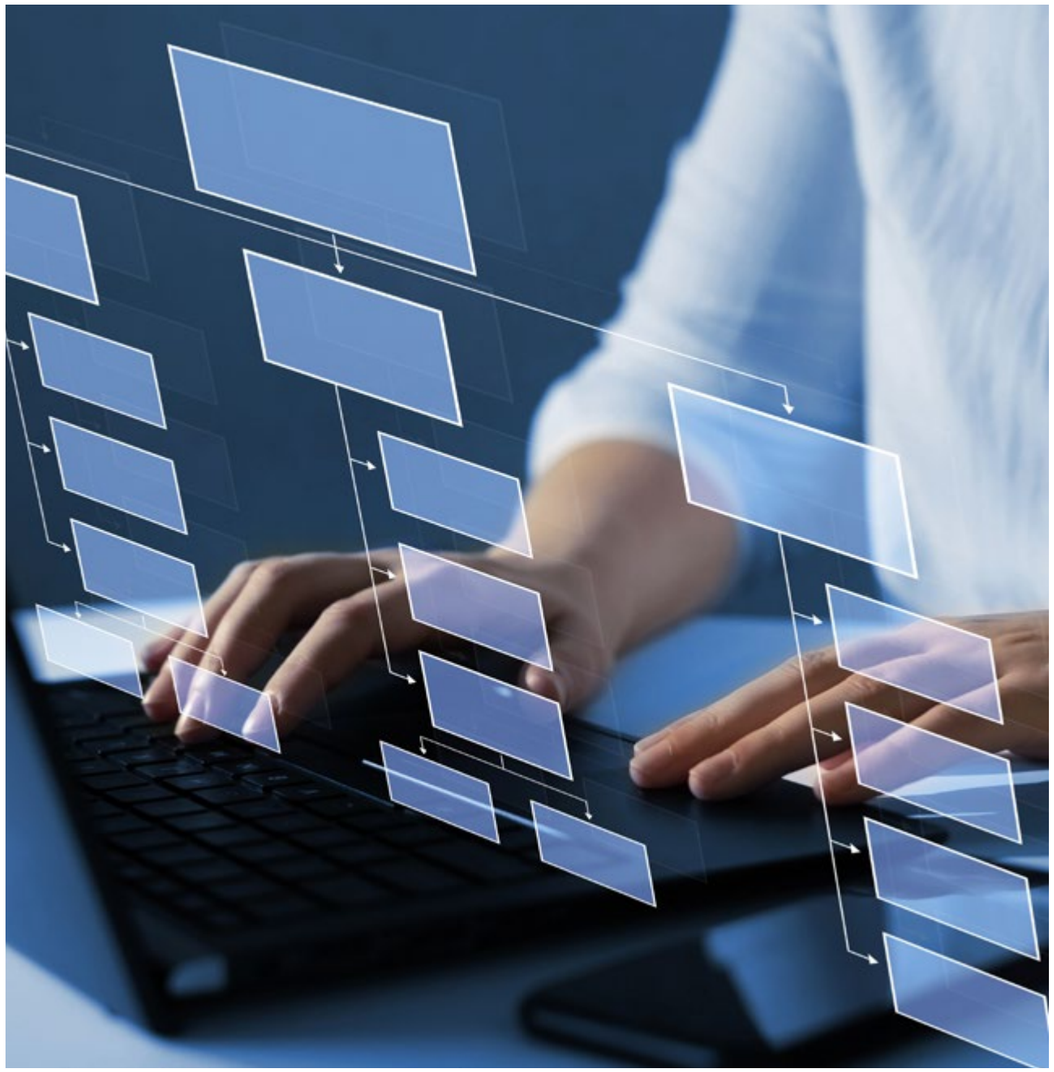
Lizenzen werden aus Sicht der Lizenzgeber meist auf Basis der gesamten Organisation (d.h. der Hochschule) beschafft und verrechnet. Das Lizenzmanagement sollte zentral in der Hochschule verankert sein und eng mit weiteren Bereichen kooperieren, z.B. der Beschaffung, dem Vertragsmanagement, der Rechtsabteilung und den dezentralen Ansprechpartnern für Softwarelizenzen, gerade im Hinblick auf die steigende Komplexität der Verträge und die hohe Geschwindigkeit an Änderungen bei Cloud-Leistungen. Ohne eine zentrale Koordinationsstelle und klare Prozesse sind die Hochschulen kaum in der Lage, entsprechend zu reagieren.

Betrachtet man die Vielzahl an Lizenztypen und Systemen, gerade bei einer Verteilung über die Hochschule, ist es meist unmöglich, eine vollständige technische Erfassung der Lizenzen durchzuführen (ein Beispiel wäre, den Zugriff auf die Ressource nur per SSO, d.h. mit Account der Hochschule zuzulassen – dies würde eine Nutzung jenseits davon unterbinden). Entsprechend benötigt man eine mit der Hochschulleitung ab-

gestimmte Strategie, um die Optimierung der Lizenzierung voranzutreiben. Cloud-Leistungen bieten den Vorteil eines transparenten Online-Managements, das jedoch entweder nur zentral betrieben werden kann seitens des Anbieters oder aufgrund einer Optimierung der Lizenzierung zentral verantwortet werden sollte. Lizenzbilanzen über Software Asset Management Tools bzw. die gegebenen Systeme an der Hochschule (z.B. im Einkauf) sind ebenso Teil des Lizenzmanagements.

Das Controlling im Lizenzmanagement sollte Governance, Compliance und Wirtschaftlichkeit stets im Blick halten: Wer benötigt wann eine Lizenz? Wie können Lizenzen ressourcenschonend weitergegeben werden? Wie kann intern eine Kostenverrechnung stattfinden?

Automatisierte Prozesse für Lizenzvergabe und -entzug sowie Reporting sollten – wo möglich – umgesetzt werden, um Ressourcen zu sparen. Manuell ist diese Arbeit, gerade an großen Hochschulen, kaum stemmbar und viel zu teuer. Verteilsysteme für Lizenzen (z.B. Shop-Systeme, Marketplace) sind mitzudenken. Das technische Lizenzmanagement (siehe 4.4) ist daher so früh wie möglich in die Prozesse einzubinden, um den Lifecycle von Lizenzen (Anfrage, Einkauf, Beschaffung, Zuweisung, Nutzerwechsel/Ressourcenwechsel, Stilllegung) organisatorisch und technisch aufeinander abstimmen zu können.



3.4.2. Transformation von On-Premises- in Cloud-Lizenzen

In der aktuellen Situation werden viele Hochschulen damit konfrontiert, dass bisherige On-Premises-Lizenzen zukünftig in der Cloud verwaltet werden, sofern die Nutzung on-premises überhaupt noch möglich ist. Hier muss also eine Transformation im Lizenzmanagement stattfinden in Bezug auf aktuell verwendete Lizenzen.

Organisatorisch und technisch ist diese Transformation ähnlich zu behandeln wie die Einführung einer komplett neuen Cloud-Leistung, inkl. entsprechender Kommunikationsmaßnahmen und Prüfungen.

Ist der Schritt in die Cloud bei der Leistung nicht gewünscht, sind die entsprechenden Verträge zu prüfen, ob eine (vorzeitige) Vertragskündigung überhaupt möglich ist.

Transformationen von On-Premises-Leistungen in die Cloud finden z.T. schrittweise statt, z.T. abrupt und innerhalb laufender Verträge. Diese Umstellungen müssen vertraglich und im Lizenzmanagement geprüft werden. Aber auch für das organisatorische und technische Lizenzmanagement ergibt sich Handlungsbedarf (z.B. durch Umstellungen von Lizenzmetriken, Laufzeiten, technische Anbindungen). Dies kann auch in einer abschließenden Bewertung zur Einstellung/Stilllegung eines Dienstes führen.

ArcGIS der Firma ESRI
Zentral stand früher eine Konsole für die Erzeugung von On-Premises-Lizenzen für die Hochschule zur Verfügung. Seit einigen Jahren läuft parallel dazu eine weitere Konsole für das Management der Lizenzen, wobei diese Lizenzen mit einem Account in der Cloud aktiviert werden und Daten der Nutzenden in der Cloud gespeichert werden. Nach und nach werden nun Lizenzen und Produktumfang in der On-Premises-Konsole eingeschränkt und mittelfristig eingestellt.

Adobe
Beim Wechsel zum neuen ETLA-Vertrag von Adobe wurden nicht nur Cloud-basierte Leistungen hinzugefügt, sondern die Lizenzvergabe vollständig auf eine nutzerbasierte Lizenzierung in der Cloud umgestellt. Das stellte die Hochschulen vor große Herausforderungen.

Sophos in NRW
Während der Laufzeit des NRW-Rahmenvertrags mit Sophos wurden Funktionen (hier: Enterprise Console on-oremises) eingestellt, sodass ein Wechsel in Cloud-only-Leistungen, oder eben ein Anbieterwechsel, notwendig war.

3.4.3. Lizenzmanagement und Community Cloud

In einer Community-Cloud-Lösung sind nicht alle verwendeten Leistungen „open source“ und ohne Lizenzkosten zu nutzen. Als Dienstleister einer entsprechenden Community-Cloud-Leistung sollte der vollständige Stack betrachtet werden, der zur Erbringung der Community-Cloud-Leistung notwendig ist: Ist hier die Nutzung durch hochschulexterne Personen erlaubt und falls ja, in welchem Umfang? Ggf. müssen hier separate Lizenzen beschafft werden. Gibt es Add-on-Lizenzen für bestimmte Produkte und wie werden diese verwaltet?

Gerade Community-Cloud-Leistungen erreichen vermutlich oft eine Größe, die ohne „Enterprise“-Features nicht mehr sinnvoll betrieben werden kann, z.B. in Bezug auf die Anbindung ans IAM (Identity & Access Management).

Das Lizenzmanagement bildet (wie bei Public-Cloud-Leistungen) hier oft die Grundlage für nutzungsbezogene Abrechnungen. Daher kann es z.B. notwendig sein, ein entsprechendes Management einzuführen, ohne dass tatsächliche Lizenzkosten vorhanden sind.

3.5. Zentrale Steuerung von Anfragen zur Nutzung von Cloud-Leistungen

Anfragen zur Verfügbarkeit und zum regelkonformen Einsatz von Cloud-Leistungen, aber auch generell zu Software werden in den meisten Hochschulen an zu vielen verschiedenen Stellen bearbeitet. Das führt zu unkoordinierten und mitunter gar falschen Antworten und zu Unzufriedenheit bei den Anfragenden. Eine zentrale und sachkundige Ansprechstelle kann hier die Servicequalität erheblich steigern – beginnend mit Anfragen bzw. dem Wunsch nach einer neuen Cloud-Leistung oder einer Anwendung, die eine Cloud-Leistung beinhaltet.

Diese Ansprechstelle muss in der Lage sein, die vielfältigen Anfragen zu steuern, Informationen bereitzustellen und so die notwendigen Schritte zur weiteren Bearbeitung zu unterstützen, nachzuverfolgen und zu dokumentieren. Ebenso ist es ihre Aufgabe, zwischen Souveränitäts- und Sicherheitsaspekten sowie Fragen der Qualität und Usability abzuwägen und zu beurteilen, welche weiteren Stellen involviert werden müssen. Sofern eine hochschulübergreifende Koordinationsstelle eingerichtet wurde, bildet die interne Ansprechstelle das Bindeglied, um bspw. Beschaffungsbedarfe zu bündeln, und sie ist insbesondere für die übergreifende kooperative Zusammenarbeit zuständig (siehe auch Wissenschaftsrat, 2023).

Eine zentrale Koordination zur Steuerung von Anfragen, insbesondere zu Cloud-Leistungen, soll hingegen nicht dazu führen, dass die Nutzenden im Einzelfall nicht mehr zu prüfen haben, ob und unter welchen Rahmenbedingungen die zur Verfügung stehende Cloud-Leistung auch tatsächlich eingesetzt werden kann und darf. Die zentrale Ansprechstelle übernimmt in diesem Rahmen eine unterstützende und beratende Rolle gegenüber den Nutzenden.
Die Aufgaben einer zentralen Ansprechstelle können je nach Governance und Prozessablauf in der jeweiligen Hochschule unterschiedlich ausgeprägt sein. So könnten dort folgende Aufgaben verortet sein:

- Steuerung/Bündelung von Anfragen
- Überblick über zentral bereitgestellte Cloud-Leistungen (und weitere Softwareverträge) sowie deren Nutzungsbedingungen und Einsatzmöglichkeiten
- Beratung über vorhandene Cloud-Leistungen und mögliche Alternativen
- Nachverfolgung und Dokumentation der Anfragen
- Beratung zu sinnvollen Lizenzierungsmodellen (organisatorisches Lizenzmanagement)
- Compliance-Regeln einhalten; Auditsicherheit unterstützen
- Unterstützung bei dezentral beschafften Lösungen, z.B. hinsichtlich Risikoabschätzungen, Exit-Szenarien
- Einhaltung von strategischen Zielen der Digitalisierung und Nachhaltigkeit im Blick halten (Ressourcenverbrauch, Souveränität, Lieferketten etc.)
- Beschaffungswege und Zahlungsmodalitäten abklären/vorschlagen
- Vorbereitung von Vertragsverhandlungen; Vertragsmodalitäten bewerten
- Vertragslaufzeiten im Blick halten
- frühe Beurteilung, ob Datenschutz, Informationssicherheit und/oder Rechtsabteilung involviert werden müssen
- Mitarbeit in übergreifenden Hochschulvorhaben zu kooperativer Softwarebeschaffung und -bereitstellung bzw. entsprechenden Cloud-Rahmenverträgen
- Kataster für (Cloud-)Software
- Bereitstellung der Nutzungsbedingungen des Anbieters sowie der hochschulinternen Ergänzungen (z.B. Entzug der Lizenz bei Inaktivität, interne Verrechnung für bestimmte Gruppen)
- Aufklärung der Nutzenden (Awareness, Schulungen)

RWTH Aachen (in Planung)

Im Rahmen der Cloud-Strategie der RWTH Aachen ist geplant, eine zentrale Cloud-Koordination am IT Center einzurichten, die u.a. folgende Aufgaben hat:

- Koordination von Community-Cloud-Technologien und Unterstützung bei deren Einbindung in die Prozesse der Hochschule
- Koordination und Einführung von Public-Cloud-Technologien, die von der gesamten RWTH genutzt werden können, und deren Einbindung in die Prozesse der Hochschule (Diese Aufgabe wird nicht ausschließlich durch das IT Center ausgeführt werden.)
- Erstellung von Hilfestellungen zur Einführung von Cloud-Technologien und Integration in die bestehenden Hochschulprozess
- allgemeine Beratungs- und Schulungsangebote zu den an der RWTH angebotenen Cloud-Technologien
- Fortschreibung der Cloud-Strategie und der daraus resultierenden Aufgaben
- Koordination der Bereitstellung von Private- und Community-Cloud-Technologien

Dabei werden auch Strukturen außerhalb des IT Centers zu diesen Aufgaben hinzugezogen.

Universität Bonn (in Planung)

Im Rahmen der aktuellen Entwicklung einer universitätsweiten Cloud-Strategie wird an der Rheinischen Friedrich-Wilhelms-Universität Bonn auch eine zentrale Cloud-Stelle ausgearbeitet und etabliert. Sie soll (aktueller Arbeitsstand) als zentrale Einrichtung innerhalb der Universität Bonn sieben zentrale Aufgaben übernehmen und verantworten:

1. Unterstützung der Fakultäten und vor allem deren Digitalisierungs-Manager:innen
2. Unterstützung bei der Marktrecherche innerhalb des Bedarfsmanagements
3. Unterstützung bei der Beurteilung und zu Empfehlungen innerhalb des Bedarfsmanagements
4. Beurteilung und Empfehlungen bei Cloud-Anträgen für kleine bzw. nicht universitätsweite Bedarfe
5. Unterstützung innerhalb des Beschaffungsprozesses
6. Unterstützung der Gremien, vor allem von Rektorat, Personalvertretung, Beauftragte für Datenschutz
7. Marktbeobachtung und Forschung zu neuen Entwicklungen im Cloud Computing und bei den Cloud-basierten Diensten

Dies soll im Genehmigungs- und Beschaffungsprozess folgende Aktivitäten einschließen:

- Beratung von anfragenden Nutzenden aus Forschung, Lehre und Verwaltung, die Interesse an Cloud-basierten Diensten haben
- Entwicklung und regelmäßige Überprüfung und Aktualisierung von Handreichungen, wie der Cloud-Checkliste, Vorlagen für die finanzielle Berechnung der Gesamtkosten, Vertragsvorlagen, Positiv- und Negativlisten
- Unterstützung bei der Ausarbeitung eines Antrags für die Genehmigung eines Cloud-basierten Dienstes
- Beratung zum richtigen Einsatz von Diensten auf der Positivliste
- Recherche zu existierenden Alternativen, die schon an der Universität Bonn genutzt werden
- Recherche zu potenziellen Alternativen, die noch nicht an der Universität Bonn genutzt werden
- Erstellung einer Abschätzung der technologischen, finanziellen und organisatorischen Folgen und Ressourcenbedarfe
- Erstellung einer Risikoabwägung zur Begutachtung durch Rechtsexpertise und Datenschutz
- Erstellung einer Empfehlung für eine Beschlussfassung durch die zuständigen Gremien
- Erarbeitung von Vorschlägen und Konzepten zur Weiterentwicklung der bestehenden Cloud-Dienste, ihres Funktionsumfangs und ihrer Einbettung in die Gesamt-IT-Infrastruktur der Universität
- Analyse von aktuellen und zukünftigen Entwicklungen der genehmigten Cloud-basierten Dienste
- Analyse von aktuellen und zukünftigen Entwicklungen von genutzten IT-Services hinsichtlich Cloud-basierter Migrationen
- Analyse von aktuellen und zukünftigen Entwicklungen von Vertragsbedingungen zu Cloud-basierten Diensten
- Analyse von aktuellen und zukünftigen Entwicklungen von Gesetzes-, IT-Sicherheits- und Datenschutzregelungen zu Cloud-basierten Diensten

.

Universität Hamburg

Das Softwareteam der Universität Hamburg (UHH) ist für sämtliche Softwarebestellungen der Single Point of Contact. Das Team prüft bei Cloud-Bestellungen primär:

- Gibt es alternative IT Services, die an der UHH genutzt werden und die gewünschten Funktionen abbilden?
- Gibt es eine Alternative auf dem Markt, die dem Datenschutz eindeutiger gerecht wird und die gleiche benötigte Funktionalität liefert?
- Werden Informationen zum Datenschutz (z.B. Whitepaper) bereitgestellt? Angaben wie „100% datenschutzkonform" sind kritisch zu betrachten.
- In welchem Land sitzt der Anbieter und werden Daten außerhalb von EU/EWR verarbeitet?

Der Antragsteller erhält die in Zusammenarbeit mit dem Datenschutz erstellte Cloud-Checkliste. Davon abhängig ergeben sich die nächsten Schritte. Aus der Erfahrung heraus werden Einschätzungen abgeben, ob die Freigabe erteilt und somit die Beschaffung eingeleitet werden kann.

Findet allerdings eine Datenverarbeitung in größerem Umfang statt (z.B. Daten von Studierenden), wird die Checkliste an die Fachkolleg:innen weitergeleitet. Das Prüfverfahren für Cloud-Dienste umfasst zurzeit folgende Maßnahmen:

- Cloud-Checkliste und AVV
- Prüfung des Bedarfs und Bestätigung durch das Digital Office gegenüber Datenschutz/Informationssicherheit
- Prüfung der Anlage im AVV von IT-Sicherheit
- Mitbestimmung (§ 88 Abs. 1 Nr. 32 HmbPersVG): Sollte ein MBR (Mitbestimmungsrecht) bestehen, kann die Mitbestimmung mit der gemäß Ziffer 4. (2) der Rahmendienstvereinbarung „Datenschutz bei Personaldaten" notwendigen Erörterung verbunden werden. Besteht kein MBR, ist für die Mitteilung an die Personalräte keine Einbindung von Abt. 6 erforderlich, sodass die zuständigen Personalräte für die Erörterung direkt von der Fachabteilung kontaktiert werden können mit der Bitte um Mitteilung, ob Erörterungsbedarf besteht. Anders als die Mitbestimmung erfordert die Erörterung keine Zustimmung der Personalräte.

Sofern der Einsatz einer universitätsweiten Cloud-/Saas-Lösung beantragt wird, liegt hier die Steuerung beim DigitalOffice. Das erweiterte Prüfverfahren mündet dann in eine Präsidiumsvorlage und wird dort entschieden und ggf. freigegeben.

4. Changes – Änderungen in Bereitstellung und Betrieb

Die zunehmende Nutzung von Cloud-Leistungen hat zweifellos die Art und Weise, wie Hochschulen ihre IT-Infrastrukturen verwalten, transformiert.

Ein zentraler Aspekt dieser Transformation ist die Frage, ob die Bereitstellung von Cloud-Leistungen tatsächlich weniger Arbeit bedeutet, wie oft angenommen wird, oder ob sie eher (temporär) eine Zunahme von Aufgaben mit sich bringt. Gerade SaaS-Lösungen (Software-as-a-Service) verlagern Verantwortung und Aufgaben von der IT auf die Nutzenden, die benötigten Kompetenzen verändern sich.

Ein weiterer Kernpunkt ist daher die Frage, welche Kompetenzen genau für die effiziente Nutzung von Cloud-Leistungen erforderlich sind. Hierbei wird beleuchtet, ob es sich um völlig neue Fähigkeiten handelt oder ob bestehende Qualifikationen und Prozesse lediglich angepasst werden müssen.

Eine weitere Herausforderung ist die Notwendigkeit, produktbezogenes technisches Wissen zu erlangen, das über den Betrieb von Anwendungen hinaus geht.

Um hier langfristig Kompetenzen aufzubauen und zu erhalten, muss bereits die interne Aus- und Weiterbildung in Hochschulen ansetzen, um sicherzustellen, dass Mitarbeitende aller Bereiche, aber insbesondere aus der IT über die erforderlichen Fähigkeiten verfügen.

Es stellt sich dennoch die Frage, inwieweit Hochschulen internes Wissen aufbauen sollten (und können) und in welchem Maße externe Unterstützung eingeholt werden sollte.

Schließlich muss die Organisation ihre Abläufe und Ressourcen entsprechend ausrichten, um sicherzustellen, dass Beschaffungsprozesse innerhalb festgelegter Zeiträume abgeschlossen werden. Service Level Agreements (SLAs) und die Vermeidung von Kompetenzverlusten bei der Verwaltung der IT-Strukturen, auch für Exit-Szenarien sind weitere Schlüsselaspekte, die in dieser Diskussion nicht vernachlässigt werden sollten.

Dieses Kapitel beschäftigt sich mit den Änderungen in den bestehenden Prozessen weitestgehend aus technischer Sicht und geht dabei auf die oben genannten Fragen ein.

4.1. Sicherheit der gespeicherten Daten

Bei der Frage, welche Risiken in Bezug auf Datenverlust und Vertraulichkeit mit der Speicherung oder Verarbeitung bestimmter Daten in einer Cloud-Leistung eingehen, steht am Anfang die Klassifikation der Daten und Workflows (ZKI, 2021).

Bei IaaS- oder PaaS-Lösungen kann dies z.T. bereits bei der Einführung durch den Serviceverantwortlichen/ „Betreiber“ bewertet werden. Bei SaaS-Lösungen liegt die Verantwortung über die gespeicherten Daten oft beim Anwendenden oder Prozessverantwortlichen selbst.

Auf technischer Ebene kann bei einer bewussten Speicherung oder Verarbeitung von Daten in der Cloud, z.B. bei der Nutzung eines Cloud-Speichers, die Einschätzung des Risikos durch den Nutzenden vorgenommen werden.

Bei einer unbewussten Cloud-Nutzung, z.B. beim Versand einer E-Mail an eine Person, die ihr Postfach in der Cloud hat, findet im Vorfeld keine Klassifizierung statt. Entsprechende Maßnahmen zum Schutz der Daten müssen hier anders stattfinden (bspw. Einzeldatenverschlüsselung).

4.1.1. Backup

Eine Datensicherung kann ein Mittel sein, um die Datenhoheit weiter zu stärken. Vorab sollte jedoch geklärt werden, welches Ziel genau in dem entsprechenden Szenario verfolgt wird:

- **Desaster Recovery und Wiederherstellung von Daten bei Ausfall oder Schäden beim Cloud Provider (bspw. Cyberangriff):** Um einem Datenverlust vorzubeugen, können Daten aus der Cloud-Leistung z.B. lokal oder bei einem anderen Cloud Provider gesichert werden. In erster Linie sollten hier zunächst die Bedingungen des Cloud Providers, z.B. hinsichtlich Verfügbarkeitszusagen oder redundanter Speicherung, geprüft werden, um die Notwendigkeit dieser zusätzlichen Speicherung zu bewerten.

- **Im Rahmen einer Exit-Strategie:** Sollte aus diversen Gründen ad hoc ein Anbieterwechsel notwendig sein, müssen die beim Anbieter gespeicherten Daten für die Hochschule verfügbar sein. Das kann z.B. durch ein regelmäßiges Backup sichergestellt werden, das dann bei Bedarf weiterverwendet wird. Hier ist zu beachten, welche Daten wie benötigt, exportiert und wiederhergestellt werden können.

- **Backup in der Cloud (IaaS/PaaS):** Als Teil des On-Premises-Notfallmanagements (Schutz gegen Zerstörung) kann der umgekehrte Weg, also ein Back-up einer lokalen Lösung in der Cloud zu speichern oder von dort wiederherzustellen, eine Möglichkeit sein, auf einen lokalen Notfall zu reagieren. Bei existenziellen Schäden wie z.B. Bränden oder bei einem Hackerangriff kann der Restore in einer Cloud-Leistung Teil der Wiederanlaufstrategie sein. Ein Cloud-Cloud-Backup, also das Back-up einer produktiv genutzten Cloud-Leistung in einer anderen Cloud, kann eine Lösung für ein Exit-Szenario oder Desaster Recovery sein.

- **Wiederherstellung von Daten bei Nutzungsfehlern:** Hier sollten zunächst das SLA bzw. die Produktbestimmungen (und Features) geprüft werden, um sicherzustellen, dass solche Fälle nicht z.B. schon in der Software-Schicht mit abgefangen werden (z.B. über Versionierung).

Folgende Aspekte sind je nach Szenario zu beachten:

- **Speicherort:** Sollen zusätzliche Sicherungen lokal oder bei einem (anderen) Cloud Provider gespeichert werden?

- **Kosten:** Die Kosten der technischen Implementierung des Back-ups können vielfältig sein. Neben den Speicherkosten (lokal sowie on-premises) fallen ggf. auch Kosten für die Datenübertragung aus der Cloud-Leistung an.

- **Formate:** Daten müssen beim Restore ggf. in einem anderen System wiederhergestellt werden können. Die Datenformate müssen entsprechend gewählt werden, damit das möglich ist. Bei Dateiformaten sind diese anders als bei virtuellen Maschinen oder Datenbanken. Bei einigen Cloud-Leistungen kann das aufgrund von stark angepassten Datenformaten schwierig bis unmöglich sein.

- **SLA/Zusicherung des Herstellers (beim Back-up in einer Cloud-Leistung):** Je nach Nutzungsszenario sind unterschiedliche Zusicherungen z.B. bzgl. Verfügbarkeit, Wiederherstellungszeiten oder Speicherdauer notwendig. Damit der Dienst einen Nutzen bringt, müssen diese im Vorfeld geprüft und angepasst gewählt werden.

Die unterschiedlichen Ziele gepaart mit den technischen Aspekten sollten in jedem Fall vor der Beschaffung von Cloud-Leistungen berücksichtigt werden.

4.1.2. Offboarding ohne Datenverlust

Bei Iaas/PaaS-Leistungen werden zwar in der Regel nicht die verwendeten Ressourcen deaktiviert, wohl aber entsprechende Berechtigungen entzogen. Hier entsteht also eine ähnliche Situation wie On-Premises.

Bei SaaS-Leistungen kann der Entzug einer Lizenz evtl. dazu führen, dass die vom Nutzenden erstellten und geteilten Inhalte verloren gehen (z.B. bei Teams, nicht aber bei SAP-SaaS). Hier müssen entsprechende organisatorische und technische Maßnahmen im Vorfeld – unter Berücksichtigung der technischen und (lizenz-) rechtlichen Rahmenbedingungen – festgelegt werden.

Berücksichtigt werden muss vor allem, dass Daten, wie z.B. Nachrichten in Kanälen oder Chats, häufig nicht oder zumindest nicht verlustfrei von einer Cloud-Lösung in eine andere Lösung übertragen werden können.

Für einzelne Nutzende gilt es zu beachten, dass erstellte und geteilte Inhalte nicht auf gemeinsam genutzten Bereichen abgelegt sein könnten, sondern in persönlichen. Dies kann dazu führen, dass mit dem Entzug der Nutzungsberechtigung bzw. der Lizenz die abgelegten Daten verloren gehen. Ein Ansatz könnte hier die Umstellung auf kostenlose Lizenzen evtl. bei gleichzeitiger Sperrung des Kontos oder die Nutzung mit Karenzzeiten sein. Letztlich verzögern diese Maßnahmen aber nur eine Löschung der Nutzerdaten.

Es bedarf also immer auch einer organisatorischen Lösung im Sinne eines geordneten Offboardings aus der Cloud-Leistung. Dieses Offboarding sollte möglichst automatisiert durch das technische Lizenzmanagement unterstützt werden, z.B. über Schnittstellen mit dem IdM (Identity Management). Zu beachten ist, dass Karenzzeiten im Zweifelsfall im Widerspruch zu bestehenden Regelungen (z.B. zur datenschutzrechtlichen Speicherbegrenzung) stehen können.

Zusammengefasst sollten folgende Punkte geprüft werden:

- Ist eine Speicherung von (geteilten) Daten in persönlichen Bereichen möglich?

- Ist es möglich, eine Karenzzeit (z.B. über einen Papierkorb) einzurichten?

- Erfolgt der Lizenzentzug manuell oder automatisch aufgrund von z.B. Rollen im IdM?

- Festlegung von Speicherrichtlinien unter Berücksichtigung der Prüfpunkte, z.B. Speicherorte für kollaborative Projekte oder Umgang mit privaten Daten.

Microsoft (OneDrive oder Teams)
Teilt ein Nutzender Inhalte aus seinem persönlichen OneDrive-Bereich mit anderen Nutzenden oder Dokumente in 1:1-Chats, so sind diese nicht dauerhaft für alle zugänglich. Verliert der Nutzende seinen Account, so sind die geteilten Inhalte für andere auch nicht mehr zugänglich.

BioRender
Bei persönlichen Abos wandern dienstliche Daten mit den Nutzenden ab. Bei einer zentralen Lizenz verbleiben diese Daten an der Hochschule, wenn der Nutzende aus der Lizenz entfernt wird.

Adobe
Adobe hat bei zentralen Verträgen umgestellt auf einen organisationsweiten Speicher und bietet keinen persönlichen Speicher mehr an; die Daten verbleiben an der Hochschule, wenn der User geht.

4.2. Servicemanagement

Mit der Nutzung von Cloud-Leistungen ändern sich auch die mit der Nutzung einhergehenden Serviceprozesse. Der Betrieb, vorher noch im direkten Zugriff in der eigenen Hochschule, befindet sich jetzt bei einem externen Cloud-Anbieter. Das hat direkte Auswirkungen auf damit zusammenhängende Entscheidungs- und Supportprozesse und auf Strukturen des IT-Servicemanagements wie das Change-Management.

Grundsätzlich bleiben Strukturen wie z.B. die Unterteilung in 1st, 2nd und 3rd Level Support erhalten, aber die genaue Ausprägung der Interaktion ändert sich – die Prozesse müssen inhaltlich angepasst werden.

Einige Beispiele können sein:

- Spezifikation der Supportwege bei unterschiedlicher Nutzung (Community-Cloud-Dienste, Public Cloud-Dienste)

- Change-Management: Der Entscheidungsspielraum, wann welche Änderungen z.B. auf Software- oder auch auf Hardware-Ebene stattfinden, ist bei der Nutzung von Cloud-Leistungen stark eingeschränkt. Anstatt Änderungen im Vorfeld zu planen, zu kommunizieren und im Zweifel genehmigen zu lassen, ist meist eher eine permanente Change-Überwachung und ein Ad-hoc-Management notwendig, um z.B. auf neue Features zu reagieren. Meist ist der Zeitraum, in dem Cloud-Anbieter Änderungen ankündigen und durchführen, deutlich kürzer als an den Hochschulen gewohnt.

- Service Level Agreements: SLAs werden vorgegeben und sind maximal über die Kosten zu steuern (z.B. höhere Verfügbarkeit oder 24/7-Support).

4.2.1. Support von Cloud-Leistungen

Dieser Abschnitt bezieht sich auf die Supportprozesse bei der Nutzung von Cloud-Leistungen. Die Rahmenbedingungen für die Einführung von neuen Cloud-Leistungen sind im 1. Ergebnisberichts der Kommission (ZKI, 2021) genannt.

Grundsätzliche Überlegungen

Bei der Beschreibung der Supportwege sollte die Rolle der IT in dem jeweiligen Szenario berücksichtigt werden:

- Vermittlung von Cloud-Leistungen externer Anbieter (Community oder Public)

- Anbieter von Leistungen für die eigene Hochschule

- Ggf. lässt sich je nach Hochschule auch noch eine dritte Rolle betrachten: Anbieter von Community-Cloud-Leistungen. Da diese aber nur für wenige Relevanz hat, wird diese Rolle im weiteren Verlauf vernachlässigt.

Diese unterschiedlichen Rollen bringen unterschiedliche Level an Support mit, der durch die IT der Hochschule geleistet wird oder werden kann. Dabei sind vor allem in der Rolle als Vermittler von Cloud-Leistungen folgende Punkte relevant:

- **Grad der Integration in die Hochschulprozesse:** Die Integration von Cloud-Leistungen in die Hochschulprozesse kann von einer reinen Authentifizierungsschnittstelle über die Übertragung von Daten zur Autorisierung bis hin zur Nutzung von Bestell- oder Abrechnungsprozessen gehen. Der unterschiedliche Grad spiegelt sich dann gleichermaßen auch im Supportumfang wider.

- **Interaktion:** Die Interaktion zwischen den lokalen Supportstrukturen (1st und 2nd Level), der eigenen IT-Administration (3rd Level) und den Cloud-Anbietern muss entsprechend geregelt und dokumentiert werden. Hier ändert sich vor allem die Rolle der IT-Administration weg vom IT-Betrieb hin zum Management komplexer Cloud-Leistungen.

- **Grenzen:** Wie viel Support der lokale 1st Level leisten muss, wie viel produktspezifisches und technisches Wissen notwendig ist und ab wann externe Unterstützung genutzt werden soll, sind keine neuen Fragen. Sie müssen aber nun gerade im Übergang 3rd Level/Cloud-Dienstleiser noch deutlicher abgegrenzt werden.

- **Dokumentation zu Funktionen bzw. Nutzung der Cloud-Leistung durch die Hochschule:** Viele Cloud-Anbieter haben bereits eine gute Dokumentation. Die identische Aufbereitung durch die Hochschule bietet hier keinerlei Mehrwert. Der Mehrwert ist nur dann vorhanden, wenn es z.B. konkrete Einschränkungen in der Implementierung der Hochschule gibt oder sich die Dokumentation auf hochschulspezifische Prozesse (vgl. oben. „Grad der Integration“) bezieht.

Aus Sicht der Nutzenden ist die große Frage, wie man den Unterschied zwischen On-Premises-Diensten und Cloud-Leistungen mit unterschiedlichen Support- und Zugriffstrukturen deutlich machen kann.

Direkter Kontakt zum Cloud-Anbieter
Teilweise können innerhalb der verwendeten Cloud-Leistung Nutzende direkt Kontakt zum Hersteller aufnehmen. Das passiert vorbei am 1st Level Support der Hochschule.

Support in kooperativen Strukturen
Grundsätzlich kann angenommen werden, dass sich die Supportwege in kooperativen Strukturen nicht gravierend von denen mit externen Anbietern unterschieden. Dennoch ist das Verhältnis unter den Hochschulen bzw. in der Community anders als gegenüber externen Cloud-Anbietern.

Bezogen auf die Supportstrukturen sind folgende Aspekte dabei zu berücksichtigen:

- **Anforderungsmanagement:** die Anforderungen, die eine Hochschule an den Anbieter einer Community-Cloud-Leistung hat, können sich z.B. auf die Verfügbarkeit aber auch auf die Kommunikation zu Changes und Wartungen beziehen. Diese sollten frühzeitig festgelegt werden, ggf. sogar in einem gemeinsamen Vertrag.

- **Betreiberkonsortium oder ein Betreiber:** Wie funktioniert der Support, wenn es nicht nur einen Community-Cloud-Anbieter gibt, sondern mehrere, die zusammenarbeiten?

- **Ausgestaltung:** Die organisatorische und technische Ausgestaltung der Supportwege obliegt dem Betreiber.

DaSi.nrw
In dem NRW Projekt Datensicherung.nrw (DaSi.nrw) gibt es mehrere Dienstgeber, die jeweils für dienstnehmende Hochschulen Back-up & Restore anbieten. In jeder dienstnehmenden Hochschule gibt es technische Ansprechpartner, die jeweils Support auf der 1st-Level-Ebene leisten. Die Eskalation in den 2nd oder 3rd Level der dienstgebenden Hochschule ist dabei möglich. Dafür wird von den dienstgebenden Hochschulen ein gemeinsames Tickettool verwendet, sodass ein gemeinsamer Support und Informationsaustausch realisiert werden können. Insbesondere für Sicherungs-Use-Cases ist die Expertise nicht auf die Dienstleister beschränkt, vielmehr können Fachleute bei den Dienstnehmern sich auch gegenseitig helfen.

Support in Interaktion mit Public-Cloud-Anbietern
Neben den allgemeinen Überlegungen sind vor allem die konkreten Supportwege bei der Nutzung von Public-Cloud-Leistungen festzulegen. Dabei geht es in erster Linie darum, wer wie mit wem spricht:

- **Kommunikationswege der Nutzenden:** Können oder dürfen die Nutzenden den Support des Cloud-Anbieters direkt kontaktieren oder müssen Anfragen über den zentralen IT-Support der Hochschule laufen?

- **Kommunikationswege für 2nd oder 3rd Level der Hochschule:** Gibt es eine Möglichkeit, für technisch versierte Anfragen aus dem 2nd oder 3rd Level der IT direkt den entsprechenden Supportlevel des Cloud-Anbieters zu kontaktieren? Um unnötige Ticket-Laufzeiten zu vermeiden, macht diese direkte Möglichkeit Sinn.

Die Fragen können dabei je nach Cloud-Leistung unterschiedlich beantwortet werden.

4.2.2. Beratung und Schulungen

Die Frage, welche Lösung für ein konkretes Nutzungsszenario die Beste ist, ist nicht neu. Durch das vergrößerte Serviceangebot im Bereich der Cloud-Leistungen wird diese Frage aber noch verkompliziert, weil neben einem Feature-Set viel mehr Kriterien einbezogen werden müssen (siehe 3).

Eine Beratung für die Nutzenden anzubieten, die diesen hilft, die richtige (Cloud-)Leistung zu finden, kann ein gutes Vehikel zur Steuerung von Anfragen sein. Dazu gehört auch eine entsprechende Dokumentation der vorhandenen Lösungen und ihrer Anwendungsgebiete. Gerade der Unterschied zwischen den Public- und Community-Cloud-Leistungen und den On-Premises-Angeboten sollte kenntlich gemacht werden (siehe 3.5).

Haben die Nutzenden die für das Nutzungsszenario beste Wahl getroffen, stellt sich vor allem bei zentral angebotenen Cloud-Leistungen die Frage nach Schulungen. Die Realisierung dieser Schulung geht Hand in Hand mit der Frage nach dem Grad der Prozessintegration und den Grenzen des Supports. So können hochschulspezifische Prozessintegrationen am besten durch diese selbst erläutert werden, für standardisierte Anwendungsszenarien gibt es im Zweifelsfall ausreichend externe Anbieter, die das Wissen dazu nicht erst aufbauen müssen. Gerade mit Blick auf den vorhandenen Personalmangel an den Hochschulen sind die Grenzen und Zuständigkeiten hier mit Sorgfalt zu wählen.

Verein zur Förderung eines Deutschen Forschungsnetzes e.V. (DFN)
Neben diversen Informations- und Austauschformaten (siehe 5.3) bietet das DFN auch anlassbezogene Workshops zu aktuellen Themen mit besonderem Augenmerk auf die Einbeziehung der nutzenden Einrichtungen. Dies kann im Vorfeld von größeren Ausschreibungen sein – bspw. OCRE – oder zu aktuellen Themen, wie zu Fragen zum Qualitätsmanagement im Zusammenhang mit Cloud-Diensten oder in krisenhaften, die Dienstkontinuität beeinträchtigenden Situationen. Die anlassbezogenen Workshops dienen auch dazu, bestehende Cloud-Angebote weiterzuentwickeln und neue Dienste zu entdecken..

4.2.3. „Ständig was Neues" – Umgang mit Updates und neuen Features, getrieben durch Cloud-Anbieter

Wie schon beim Vertragsmanagement (siehe 3.2.3) beschrieben, unterliegen Cloud-Leistungen permanenten Änderungen durch die Cloud-Anbieter, die nicht oder kaum durch die Hochschule als Kunde beeinflusst werden können.

Dadurch entsteht ein ständiger Arbeitsaufwand in Bezug auf Information, Prüfung und ggf. Anpassung von Dokumentation und Schulungsmaterial. Änderungen oder neue Features werden von den Cloud-Anbietern häufig nicht oder nur sehr kurzfristig im Vorfeld angekündigt. Dies führt dazu, dass eine Prüfung oder Konfiguration evtl. erst im Nachhinein erfolgt, und birgt die Gefahr, dass neue Features oder Cloud-Leistungen bereits genutzt werden, bevor diese Prozesse abgeschlossen sind.

Auch kann es durch nicht beeinflussbare Roll-out-Mechanismen bei Cloud-Leistungen zu unterschiedlichen Versionsständen und damit zu Unterschieden in der Bedienung bei den Nutzenden kommen.

Bei Community-Cloud-Leistungen kann hier evtl. noch Einfluss genommen werden. Bei Public-Cloud-Leistungen ist eine Lösung dieses Dilemmas aktuell nicht in Sicht.

4.3. Administration

Die Administration ändert sich in zwei Bereichen:

- Neu dazu kommen die Bereitstellung von Cloud-Leistungen und die damit verbundene Administration und Konfiguration.

- Betrieb und Bereitstellungen von Service auf Basis von IaaS/PaaS-Cloud-Leistungen

Im Folgenden werden die entstehenden (zusätzlichen) Arbeitsaufwände und ggf. neuen Kompetenzen miterörtert.

Zu beachten ist hier, dass mögliche Kompetenzverluste in der IT bzgl. On-Premises-Leistungen verhindert werden.

4.3.1. Bereitstellung von Cloud-Leistungen

Über das reine Lizenzvertragsmanagement hinaus gibt es innerhalb einer Cloud-Leistung diverse Aufgaben, die zur (zentralen) Bereitstellung innerhalb einer Hochschule anfallen:

- **Nutzermanagement:** Berechtigungen, Lifecycle, Lizenzvergabe, Anbindung an das IAM der Hochschule

- **Konfiguration:** Diese Aufgabe ist nicht neu in Bezug auf den Betrieb von Services, jedoch ändern sich ggf. Art und Umfang. Hierunter fallen z.B. auch die technische Umsetzung von Regelungen, wie die erlaubte Speicherregion, oder freigeschaltete Features.

- **Bereitstellung von Landing Zones/zentralen Leistungen:** Manche Cloud-Anbieter von IaaS/PaaS empfehlen explizit, zentrale Dienstleistungen wie VPN-Anbindung oder Monitoring an einer Stelle zentral bereitzustellen.

Darüber hinaus ist auch auf der technischen Ebene der Umgang mit Changes (siehe 4.2.3) zu prüfen. Releases können nicht einfach übersprungen werden, nicht nur bei der Nutzung von Online-Angeboten. Selbst bei lokal installierter Software passieren die Updates entweder automatisch, getriggert durch den Cloud-Anbieter, oder die Servicespanne der vorherigen Versionen wird entsprechend kurzgehalten. Zusammen mit der hohen Änderungsfrequenz und den vielen Querbezügen/Abhängigkeiten zwischen Produkten stellt das die Hochschulen vor eine große Herausforderung.

Unsere Empfehlung ist darüber hinaus, auch die angepassten Konfigurationseinstellungen in regelmäßigen Abständen (am besten automatisiert) zu prüfen.

Ähnlich wie im Servicemanagement ist auch hier zu klären, wo die technische Grenze zwischen der Hochschul-IT und dem Cloud-Anbieter gezogen wird. Entsprechend viel produktspezifisches Wissen muss hier aufgebaut oder eben extern hinzugezogen werden.

Adobe
Bei Updates wurden in der Vergangenheit regelmäßig manuell vorgenommene organisationsweite Konfigurationsänderungen zurück auf den Standard gesetzt. Diese hochschulspezifischen Einstellungen müssen also regelmäßig geprüft werden.

Microsoft M365
Updates werden zentral durch Microsoft getriggert und auch bei lokal installierten Office365-Versionen durchgeführt. Neu verfügbare Apps werden je nach Lizenzmodell automatisch für die Nutzenden bereitgestellt. Ist dies nicht gewünscht, müssen diese regelmäßig geprüft und explizit ausgenommen werden.

4.3.2. Abbildung von Leistungen auf oder mit Cloud-Infrastruktur

Cloud-Leistungen können auch verwendet werden, um auf dieser Basis Dienste für die Hochschule zu erbringen. Die Nutzung bezieht sich dabei hauptsächlich auf IaaS/PaaS Services.

Der Kauf und Betrieb der einem Dienst (z.B. einer Datenbank) zugrunde liegenden Plattform entfällt dadurch. Im Gegenzug werden Kompetenzen in der Konfiguration und Administration der Cloud-Leistung benötigt.

Die Planung und Überwachung der anfallenden Kosten für CPU, Datentransfer etc. ändert sich grundlegend. Während im On-Premises-Betrieb der Kauf der Infrastruktur eher einmalige und planbare Kosten verursacht, fallen bei IaaS- oder PaaS-Lösungen Kosten in Abhängigkeit von der Nutzung an.

Zu beachten ist auch, inwieweit Administrationswerkzeuge, Monitoring und Logging in bestehende (On-Premises-) Lösungen integriert werden können. Evtl. ist hier eine (Lizenz- oder Feature-) Erweiterung der vorhandenen Lösung oder die Nutzung neuer, vom Cloud-Dienstleister angebotener Tools notwendig.

Bei der Abbildung von Leistungen auf einer IaaS-/PaaS-Infrastruktur gilt es, wie bei anderen Cloud- Leistungen auch, Changes zu berücksichtigen. (Sicherheits-)Updates oder Feature-Änderungen werden vom Cloud-Dienstleister womöglich sehr kurzfristig oder gar nicht angekündigt und direkt umgesetzt. Sie bedürfen einer regelmäßigen aktiven Beobachtung und Prüfung der Kompatibilität zur abgebildeten Leistung.

4.4. Technisches Lizenzmanagement

Die Erfassung der Lizenzen ist die Grundlage für das technische Lizenzmanagement, um Prozesse zur Freigabe, Prüfung sowie Zuweisung/Übertragung/Entfernung von Lizenzen festlegen zu können. Für jeden Cloud-Service wird erfasst, welche Lizenzen inkl. Typen geplant oder im Einsatz sind. Auf Basis der Analyse kann anschließend nach Servicemodell (SaaS, PaaS, IaaS) und weiteren Kriterien (z.B. Softwareklassen, Lizenztypen) geclustert werden.

Das technische Lizenzmanagement klärt vor der Beschaffung, wie Lizenzen verwaltet werden (Anbindung an das Identitätsmanagement, Schnittstellen der Anbieter, Freigabeworkflows für Lizenzvergabe und -entzug, Nutzungsszenarien für „Bring your own licence“). Wird eine Software-Asset-Management-Lösung eingesetzt, stellt sich die Frage, inwieweit die Verwaltung von Cloud-Lizenzen dort möglich ist (z.B. über Schnittstellen) oder welche Alternativen es gibt. Mit dem Einkauf muss vorher geklärt sein, wie eine technische Überbuchung von Lizenzen (z.B. neue Identität = neue Lizenz) sich mit dem Beschaffungswesen vereinbaren lässt.

4.4.1. Lifecycle von Lizenzen – nutzerbezogene Lizenzen

Bei der Zuweisung von nutzerbezogenen Lizenzen gibt es zwei unterschiedliche Wege: eine regelbasierte Zuweisung für größere Nutzergruppen und individuelle/manuelle Zuweisungen für einzelne Nutzenden. Dabei gilt es, den vollständigen Lifecycle zu unterstützen:

- **Zuweisung von Lizenzen:** Eine Selbstregistrierung, automatische Zuweisung durch das IdM (basierend auf Merkmalen, Benutzergruppen o.Ä.) oder die Nutzung von Shop-Systemen sind hier Beispiele für die Realisierung.

- **Entzug von Lizenzen:** Je nach Cloud-Leistung ist hier das Thema Datenverlust (siehe 4.1.2) im Vorfeld zu klären.

- **Weitergabe von Lizenzen:** Gerade bei individueller Zuweisung und Nutzung ist dies eine Möglichkeit, um z.B. beim Ausscheiden oder Wechsel der Zuständigkeiten Lizenzen weiterzuverwenden. Durch die Bindung der Lizenz an den Nutzenden ist dieser Prozess technisch zu unterstützen und muss meist gegenüber dem Cloud-Anbieter kenntlich gemacht werden. Zu beachten sind hier vor allem geltende rechtliche Lizenzbedingungen des Cloud-Anbieters sowie organisatorische Anforderungen wie die korrekte interne Abrechnung.

Grundsätzlich sollten diese Prozesse soweit möglich automatisiert werden. Das ist nur in enger Zusammenarbeit mit dem Thema IAM (siehe 4.5) möglich.

Gleichzeitig gilt es zu beachten, ob der Cloud-Anbieter eine eigene Schnittstelle/Weboberfläche hat, über die der oben genannte Lifecycle abgebildet werden muss, oder ob lokale Mittel der Hochschule dafür verwendet werden können/müssen.

Jeder Schritt des Lifecycles sollte mit entsprechenden kommunikativen Maßnahmen begleitet werden, um für den Nutzenden Transparenz zu schaffen.

4.4.2. Lifecycle von Lizenzen – gerätebezogene Lizenzen

Bei PaaS-Leistungen ist in der Regel kein gesondertes Lizenzmanagement notwendig, da die Leistung und die Lizenz vollständig vom Anbieter bereitgestellt werden.

Bei IaaS-Leistungen hingegen kann ein Lizenzmanagement notwendig sein und Änderungen an der Infrastruktur (z.B. CPU, RAM) können Lizenzänderungen (z.B. bei der eingesetzten Datenbank) bedeuten. Gerade „Bring your own licence"-Modelle werden bei flexibler IaaS-Nutzung schnell kompliziert, bieten allerdings den Vorteil, dass spezielle Education-Konditionen oder Rahmenverträge der Hochschule direkt verwendet werden können.

Bei SaaS wird ein gerätebezogenes Lizenzmanagement häufig notwendig sein.

Es gilt, das Lifecycle Management aus mindestens zwei Blickwinkeln zu betrachten und zu unterstützen:

- Änderungen an den Lizenzen (z.B. Kündigung, Ende der Vertragslaufzeit) sollten dazu führen, dass auch die (virtuelle) Hardware außer Betrieb genommen wird.

- Änderungen an den Ressourcen können eine Nachlizenzierung erfordern.

Automatisierungsmöglichkeiten bietet hier z.B. die Nutzung einer Configuration Management Database (CMDB), in der Hardware, Lizenz und erbrachter Service definiert und verknüpft werden. Diese könnte z.B. durch Schnittstellen zum Cloud-Anbieter Transparenz über die Ressourcen in der Cloud schaffen.

Weitere Möglichkeiten bietet die Nutzung von Agents auf jedem Server, über die Informationen über die Anzahl der Cores, RAM oder Aktivitäten nachverfolgt werden.

4.5. Nutzermanagement und Auswirkungen auf die IAM-Strukturen der Hochschule

Potenziell lassen sich auch Cloud-Leistungen als Bestandteile einer modernen Lösung für Identity & Access Management (IAM) nutzen.

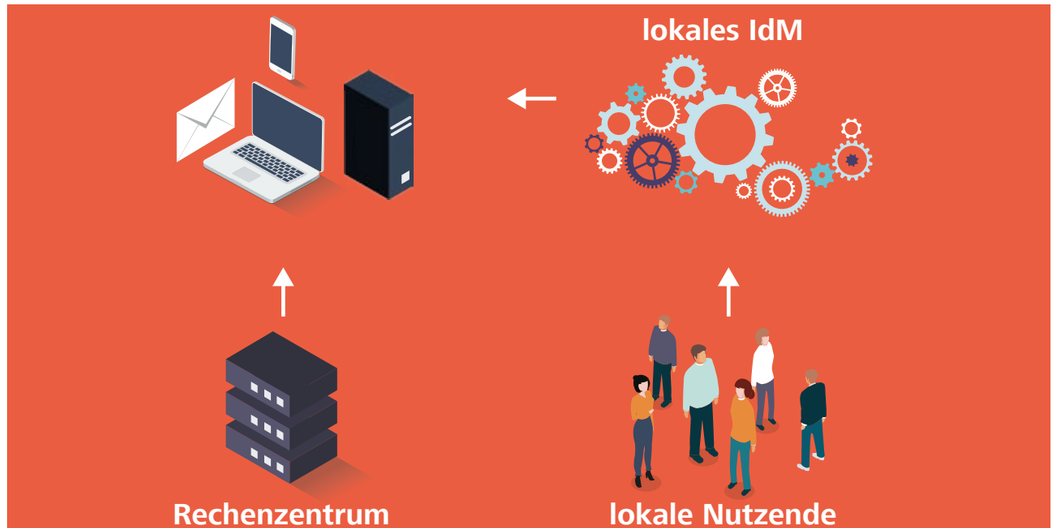


Abbildung 1: IAM in lokalen Umgebungen

Während die IAM-Strukturen bislang überwiegend auf lokale Nutzende und lokale Leistungen in der Hochschule ausgelegt waren **(siehe Abbildung 1: IAM in lokalen Umgebungen),** hat sich inzwischen die Komplexität erhöht, sowohl durch die Bereitstellung von Leistungen für Nutzende außerhalb der Hochschule als auch durch die Nutzung von Cloud-Leistungen **(siehe Abbildung 2: IAM in Multi-Cloud-Umgebungen).**

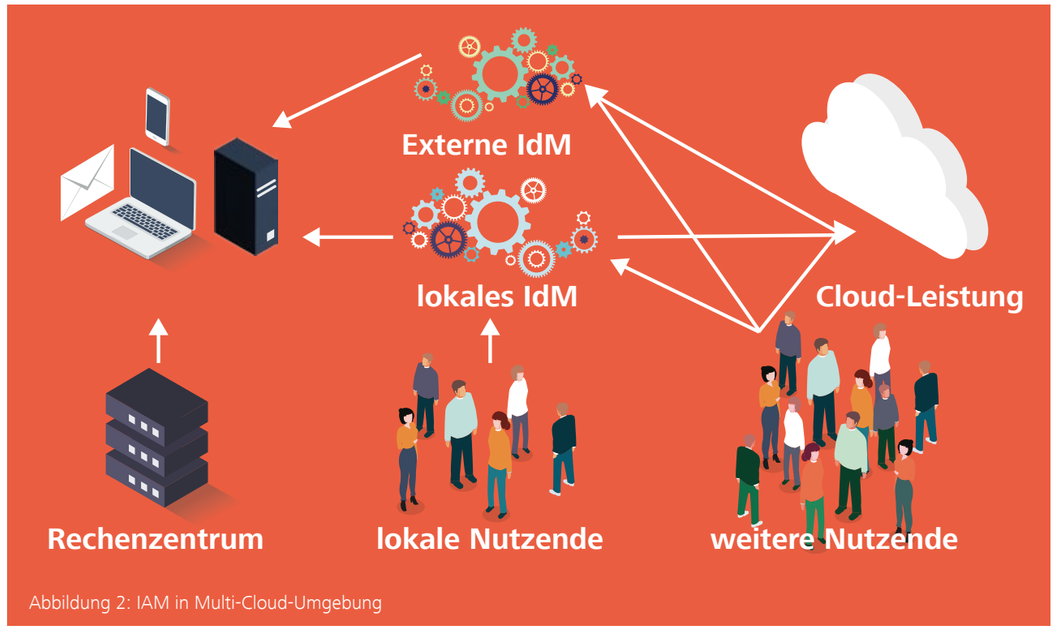


Abbildung 2: IAM in Multi-Cloud-Umgebung

Durch die sich wandelnden Anforderungen sind klassische IAM-Konzepte unter Druck geraten, dazu gehören z.B. externe Qualitätsanforderungen, Compliance-Anforderungen (Ist für jedes Konto der Bezug zur Hochschule geklärt? Werden ehemalige Mitarbeitende und Studierende zeitnah gesperrt und gelöscht? etc.), Anforderungen aus dem Lizenzmanagement und insbesondere auch die IT-Sicherheit (Multi-Faktor-Authentifizierung, zentrale Autorisierung, zentrale Nachvollziehbarkeit/Audits).

Eine übliche Basis für eine IAM-Landschaft besteht aus folgenden Elementen:

- Ein zentrales IdM bindet über Connectoren Datenquellen wie die Personalverwaltung und die Studierendenverwaltung an und verarbeitet diese Daten in automatisierten Prozessen.

- Ein zentraler Verzeichnisdienst, z.B. einem Active Directory oder einem OpenLDAP, wird durch dieses IdM verwaltet.
- Ein Identity Provider (IdP) auf Basis von Shibboleth gewährleistet ein zentrales Single Sign-on für Webdienste und stellt die Integration in Föderationen bereits, insbesondere die DFN-AAI (https://www.aai.dfn.de/) und Edugain (https://edugain.org/).

- Auch lokale Angebote werden nach Möglichkeit an den IdP angebunden.

Hochschulübergreifende Föderationen (z.B. idm.nrw, bwidm) als Basis für Community-Cloud-Dienste (wie z.B. Sciebo, bwSync&Share) definieren gemeinsame Standards z.B. hinsichtlich übergreifender Rollen („Privatdozent“), die u.U. in den lokalen IAM-Systemen noch nicht verfügbar sind und erweitert werden müssen.

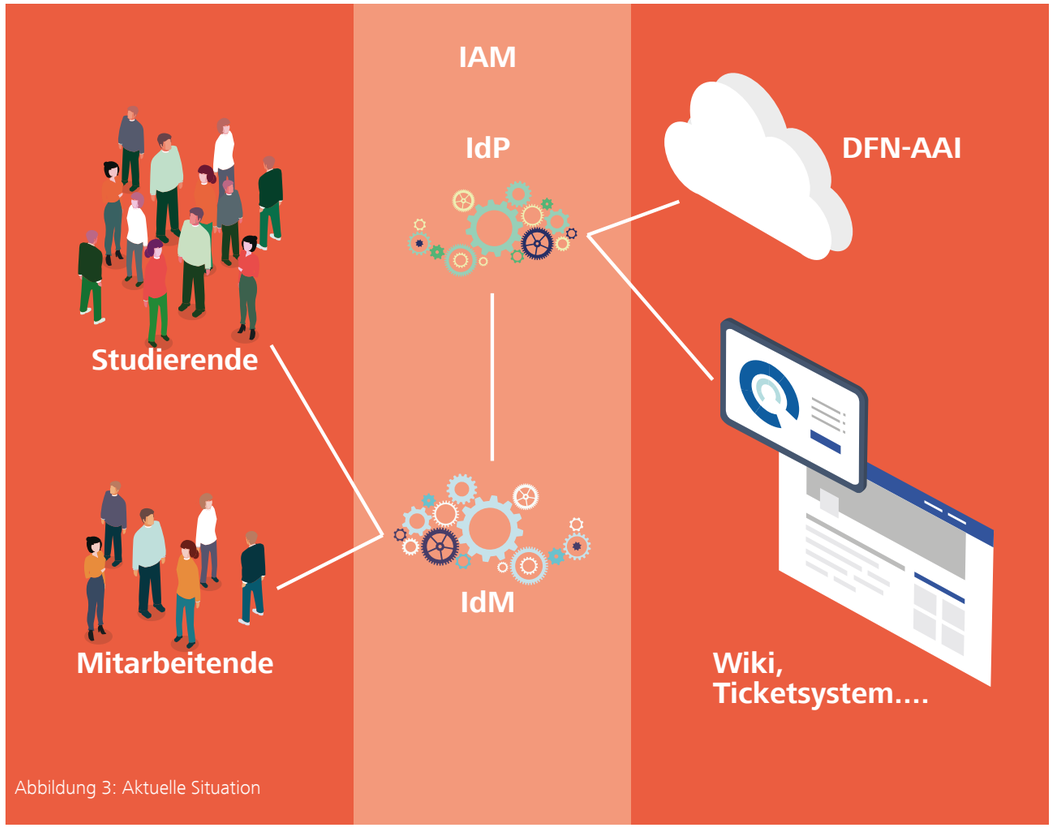


Abbildung 3: Aktuelle Situation

Neben diesen organisatorischen Anforderungen sind auch technisch neue Herausforderungen zu bewältigen, z.B. sind in der Cloud andere Schnittstellen zu bedienen als in der On-Premises-Umgebung.

Einige dieser Herausforderungen und Chancen im Überblick:

- Einführung einer modernen Multi-Faktor-Authentifizierung

- zentrale Sicherheitsrichtlinien

- zentrale Autorisierungsmöglichkeiten

- Anbindung von Cloud-Diensten z.T. über individuelle Protokolle

In der Regel wird sich eine Hochschule der Cloud-Nutzung nicht vollständig verschließen können. Abhängig von der Strategie reicht die mögliche Bandbreite von minimalem Einsatz ausgewählter Dienste über eine IAM-On-Premises-/Cloud Koexistenz bis hin zu einem denkbaren „Cloud first“-Ansatz.

4.5.1. IAM vollständig On-Premises

Auch eine vollständig on-premises betriebene IAM-Lösung kann als Basis für die Nutzung von Cloud-Leistungen eingesetzt werden. Allerdings muss kritisch hinterfragt werden, ob die gegenwärtig eingesetzte Lösung die erforderlichen Schnittstellen bedienen kann oder ob eine Erweiterung bzw. Modernisierung der IAM-Lösung notwendig wird.

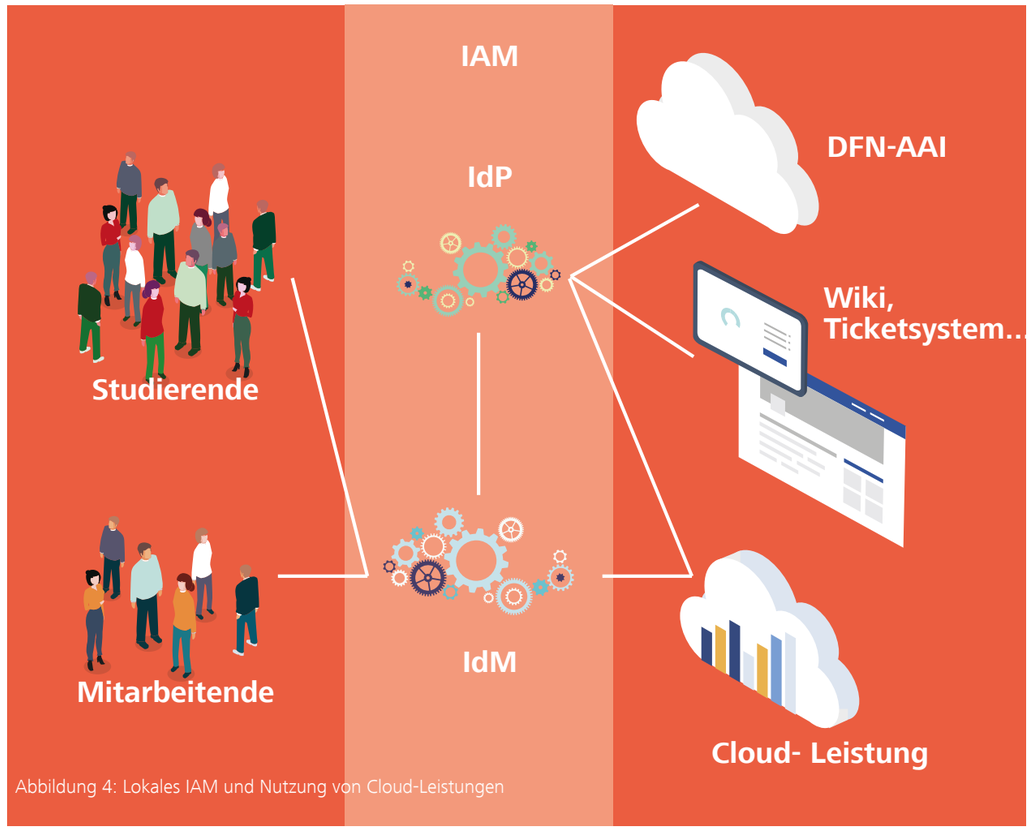


Abbildung 4: Lokales IAM und Nutzung von Cloud-Leistungen

Hinweis: Der Aufwand zur Anbindung von Cloud-Diensten kann schnell den bislang üblichen Aufwand für die On-Premises-Dienste übersteigen, insbesondere wenn der Dienst direkt und nicht über eine Föderation angeboten wird.

(On-Premises-)Anwendungen sind z.T. nicht direkt an das zentrale IAM angebunden, sondern nutzen einen Verzeichnisdienst als Multiplikator (z.B. ein LDAP oder Active Directory).

Moderne Protokolle und die Anbindung an die Cloud-Dienstleister unterscheiden sich z.T. deutlich von der bisher gelebten Praxis.Evtl. kann der für die Anbindung an die DFN-AAI eingesetzte IdP auch die Anmeldung zu Cloud-Diensten ermöglichen. Der gesamte Lifecycle ist allerdings komplex und erfordert, dass in der Cloud auch die Autorisierung, abgelegte Daten, die Lizenzvergabe, die Löschung von Konten etc. berücksichtigt werden.Moderne Authentifizierungsverfahren können durch „bedingte Anmeldungen" bzw. „Conditional Access" die Sicherheit erhöhen.

Adobe
Adobe weist in bestimmten Konstellationen automatisch jedem angemeldeten Konto eine Lizenz zu, ermöglicht dabei das Überschreiten des erworbenen Kontingents und rechnet dies nachträglich ab. Fehlende Autorisierung kann damit zu einem Kostenrisiko werden.

4.5.2. Hybrides IAM

Es gibt verschiedene IAM-Lösungen in der Cloud, die an ein lokales IAM angebunden werden können, insbesondere als Unternehmensanwendungen von Microsoft oder Google. So ist es möglich, das eigene IAM oder einen eigenen Verzeichnisdienst mit einer Cloud-(IAM-) Leistung zu synchronisieren. Dabei können z.B. durch Filter nur Teile der Konten und Gruppen synchronisiert werden, etwa alle Mitarbeitenden und keine Studierenden. Die Anmeldung in der Cloud wird so mit dem eigenen IdP verknüpft, dass die Anmeldung der Nutzenden über die bekannten Verfahren der eigenen Hochschule erfolgt.

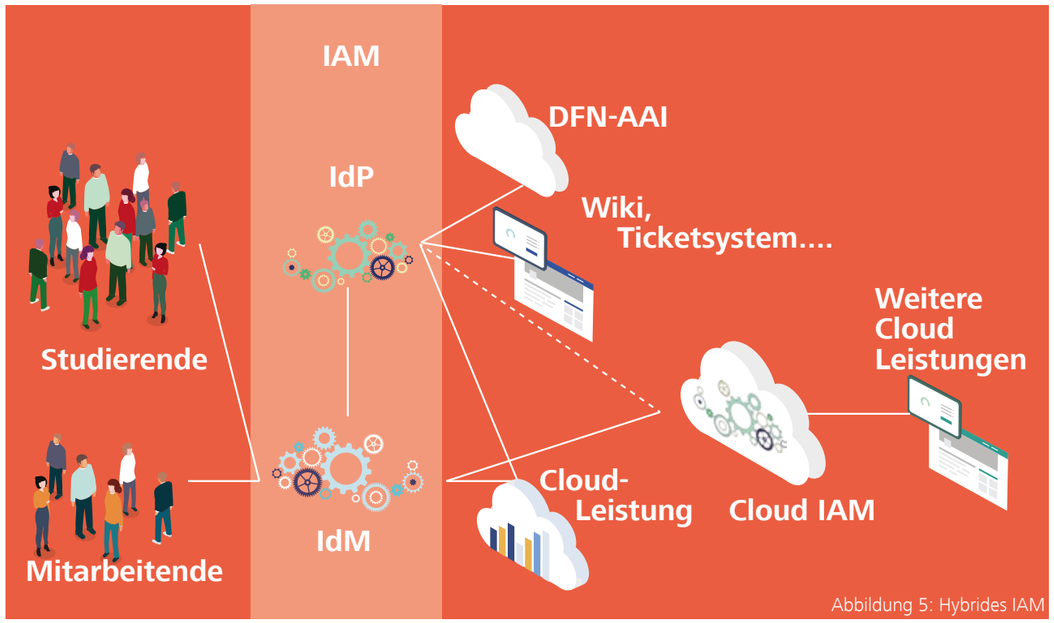


Abbildung 5: Hybrides IAM

Auf diesem Wege können dann auch weitere Leistungen an das Cloud-IAM angebunden und verwaltet werden. Für die großen Cloud-Leistungen sind diese Verfahren in der Regel gut dokumentiert.

Dabei kann die Hochschule die Nutzung auch auf einzelne Konten oder Gruppen einschränken. Eine aktive Verwaltung der Konten (Provisionierung) in den Drittsystemen kann ebenfalls umgesetzt werden, ist allerdings – verglichen mit der Anmeldung – weniger verbreitet. Die Hochschule hat über die Cloud-Verwaltungsoberflächen eine Übersicht über die angebundenen Drittsysteme, kann für die Autorisierung bereitgestellte Genehmigungsverfahren nutzen und z.T. auch Auswertungen zur Nutzung der Drittsysteme erstellen.

Es muss allerdings berücksichtigt werden, dass diese Genehmigungsverfahren zwar praktisch, aber vergleichsweise rudimentär und die Auswertungsmöglichkeiten eingeschränkt sind.

Microsoft 365
Microsoft 365 enthält einen umfangreichen Katalog an „Unternehmensanwendungen", die in gut dokumentierten Verfahren angebunden werden können und auf diesem Wege die sichere Anmeldung für Konten und Gruppen, die Lizenzverwaltung oder Provisionierung ermöglichen.
Neben Anwendungen aus diesem Katalog (Adobe, Cisco Webex, Zoom etc.) können auch weitere und eigene Anwendungen angebunden werden.

4.5.3. Perspektive: IAM als Cloud-Leistung

Bei der skizzierten Hybrid-Anbindung zu einem Cloud-IAM-Dienstleister kann ein Teil der Dienste sowohl an den lokalen IdP als auch an den IdP des Cloud-IAM-Dienstleisters angebunden werden. Damit wird sich dann ab einem gewissen Punkt die Frage stellen, ob eine Konsolidierung auf nur einen IdP, in der Regel den Cloud-IdP, anzustreben ist. In der Regel wird dies für Hochschul-interne Dienste möglich sein, allerdings ist ein IdP eines Cloud-IAM-Dienstleisters meist nicht föderationsfähig und kann so nicht direkt an Föderationen wie die DFN-AAI oder die Landesföderationen angebunden werden.

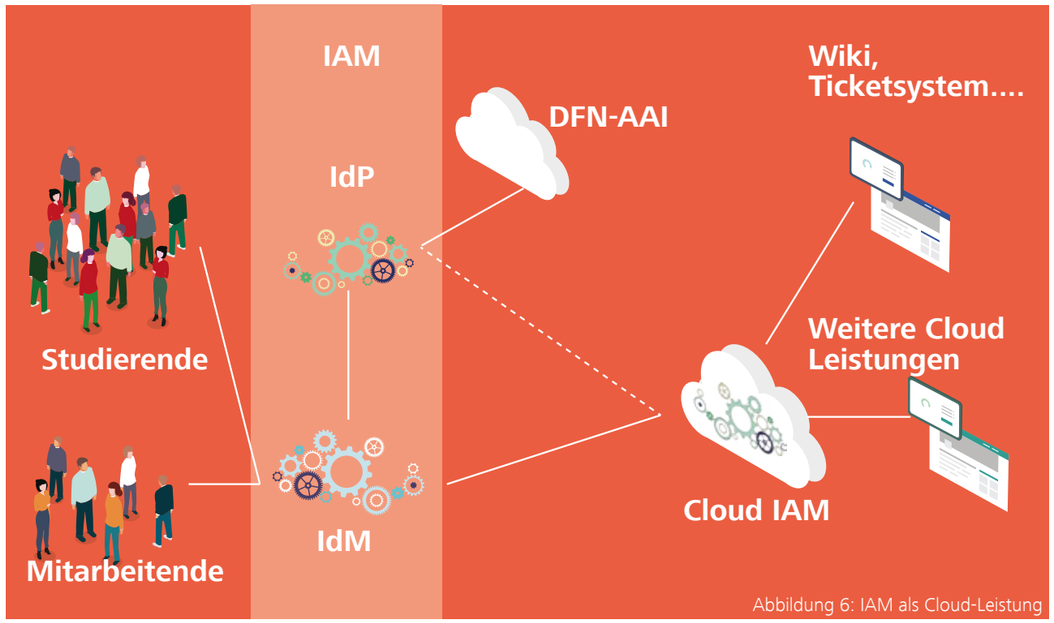


Abbildung 6: IAM als Cloud-Leistung

Auch wenn Vorteile in der Konsolidierung auf einen Cloud-IdP gesehen werden, wird der Betrieb eines eigenen IdPs, ggf. reduziert auf eine Rolle als Gateway in die Föderationen, weiterhin erforderlich sein.

5. Anhang

5.1. Mitglieder der ZKI-Kommission Cloud

Denise Dittrich	Leitung der Kommission Cloud stellv. Abteilungsleitung Systeme und Betrieb, IT Center, RWTH Aachen University
Elke Spanke	stellv. Leitung der Kommission Cloud Business Relationship Managerin, Stabsstelle Digital Office, Karlsruher Institut für Technologie (KIT)
Birgit Alkenings	Beschaffung von Software-Lizenzen, Heinrich-Heine-Universität Düsseldorf
Hansjörg Ast	Universität Frankfurt
Nicole Bargsten	Teamleitung Lizenzmanagement, IT.SERVICES, Ruhr-Universität Bochum
Dirk Bei der Kellen	Cloud Servicemanagement, DFN
Kerstin Bein	Universität Mannheim
Bernd Beining	Sprecher ZKI AK Softwarelizenzen, Hochschule Osnabrück
Irmgard Blomenkemper	Universität Köln
Ingrid Bohr	Kooperationsunterstützung bwUni.digital
Bernhard Brandel	Kath. Universität Eichstätt-Ingolstadt
Oliver Diekamp	Universität München
Peter Dräxler	Universität Kassel
Malte Dreyer	HU Berlin
Angela Ebert	Fachliche Leitung Software RRZ, Universität Hamburg
Nadine Fritz	Koordinatorin HITS IT-Beschaffung Bayern, Universität Augsburg
Christian Fötinger	Hochschulübergreifender IT Service Informationssicherheit (HITS IS/ISMS Consulting) des bayerischen Digitalverbunds Technischen Hochschule Augsburg
Jacqueline Gerland	Arbeitsgruppenleitung IT-Nutzer:innenservice, Universität Kassel
Patrick von der Hagen	Karlsruher Institut für Technologie (KIT)
Erik Hecht	Universität Köln
Michael Heckel	IT Unit, Technische Universität Nürnberg (UTN)
Robert Hellwig	Universität Siegen
Margitta Höftmann	Universität Weimar
Gernot Kirchner	Technische Universität Chemnitz, Stabsstelle Datenschutzbeauftragter/Juristische Angelegenheiten
Sebastian Klepatz	TU Clausthal
Nikolaj Kopp	GWDG Göttingen
Frederik Krist	Universität Mannheim
Eberhard Kurz	Universität Gießen
Camilo Lara	Goethe-Universität Frankfurt am Main
Alejandra Lopez	Universität Duisburg-Essen
Christian Meyer	Cloud Servicemanagement, DFN
Andreas Michels	Universität Duisburg-Essen
Thorsten Michels	RPTU Kaiserslautern-Landau
Timo Nogueira Brockmeyer	Universität Osnabrück
Manfred Paul	Hochschule München
Kai Philipp	Universität Frankfurt
Torsten Prill	Freie Universität Berlin ZKI e.V: CEO
Andreas Röber	Universität Kassel
Maja Ruby	Landtag Rheinland-Pfalz
Anna Schindler	TU Darmstadt
Christian Schultz	Technische Universität Dortmund
Thomas Schuster	Koordinator Campus IT, Hochschule Pforzheim
Julia Seidel	Koordinatorin HITS IT-Beschaffung Bayern, Universität Würzburg
Michael Stern	Hochschule Bremen
Christian M. Stracke	Koordinator Cloud-Strategie, Universität Bonn
Dirk von Suchodoletz	Co-Direktor RZ, IaaS/OpenStack, Universität Freiburg
Jens Syckor	Datenschutzbeauftragter, TU Dresden
Alexander Terecik	Projektkoordination H3 (Digitalpakt), Universität Kassel
Laura Thompson	Universität Frankfurt
Henry Trobisch	Hochschule Osnabrück
Thomas Vetter	Universität Kassel
Jan Waschkuhn	Universität Frankfurt
Gina Weiland	zentrale Softwarebeschaffung und Leitung 1st Level Support, Universität Trier (ZIMK)
Malte Wilhelm-Bachmann	Universität Hamburg
Bert Zulauf	Universität Düsseldorf

5.2. Weitere Begriffsklärung

Der Cloud-Begriff umfasst sehr unterschiedliche Ausprägungen, die in der Praxis anhand von zwei Dimensionen genauer definiert werden können: Zum einen kann unterschieden werden, wie die Dienstleistung definiert wird, zum anderen ist oft das genauere Verhältnis zwischen Anbieter und Kunde zu unterscheiden. Anhand dieser Dimensionen können sich unterschiedliche Schwerpunkte ergeben, die bei der weiteren Befassung betrachtet werden müssen.

In der ersten Dimension wird in der Regel unterschieden in „Infrastructure as a Service" (IaaS), „Plattform as a Service" (PaaS) oder auch „Software as a Service" (SaaS).

IaaS umfasst dabei z.B. virtuelle Maschinen und Speicherdienste, die ein Kunde mieten kann, um damit selbst eine hochverfügbare Datenbank zu realisieren, die wiederum als Basis für eine Anwendung wie Nextcloud dient. Möchte man nicht selbst eine hochverfügbare Datenbank betreiben, kann man diese auch als typische PaaS-Cloud-Dienstleistung einkaufen und reduziert so einen Teil des Betriebsaufwands. Die Option, den Betrieb einer Nextcloud-Anwendung als Cloud-Dienstleistung einzukaufen, ohne sich selbst mit Serverbetrieb, Datenbankbetrieb etc. zu beschäftigen, ist ein typisches Beispiel für eine SaaS-Cloud-Dienstleistung.

Mit der Dimension des Betreibers ist der erste Gedanke oft die „Public Cloud", bei der ein externes Angebot einem unbeschränkten Kundenkreis zur Verfügung steht, z.B. als Angebot der sogenannten Hyperscaler. In diesem Fall betreibt der Kunde bspw. keine eigene Infrastruktur und verlagert sämtliche betrieblichen Aspekte zum Anbieter, gleichzeitig stellen sich hier insbesondere Fragen zum Datenschutz, zur Souveränität etc. Der Gegenentwurf ist eine „Private Cloud", bei der eigene Infrastruktur On-Premises aufgebaut und betrieben wird, die aber Leistungen nach Cloud-Standards bereitstellt, z.B. bestehend aus lokalem S3-Speicher, einer Laufzeitumgebung für Container.

Das ermöglicht z.B. eine zeitgemäße Anwendungsentwicklung und einen zeitgemäßen Anwendungsbetrieb auf lokalen Umgebungen, insbesondere auch für Daten, die aufgrund von Datenschutz oder Vertraulichkeit nicht für die Verarbeitung in einer Public Cloud zugelassen sind.

Als mögliche Abstufungen und Kombinationen existiert zunächst der Begriff der „Hybrid Cloud", bei der eine eigene Private Cloud mit einer Public Cloud gekoppelt wird, bspw. um lokale Kapazitäten mit Leistungen der Public Cloud zu ergänzen oder nach anderen Kriterien zu optimieren. Unter einer „Multi Cloud" versteht man die Situation, in der ein Kunde mehrere Anbieter auch für ähnliche Cloud-Dienstleistungen verwendet. Die strategische Entscheidung, Anwendungen bei verschiedenen Cloud-Anbietern zu betreiben und sich die Möglichkeit offen zu halten, diese Anwendungen zwischen den Anbietern zu verschieben, ist für IaaS und PaaS aufgrund ähnlicher Angebote realistisch und reduziert die Abhängigkeit von einzelnen Anbietern und damit existierende Risiken bei Änderungen der Konditionen, bei rechtlichen Rahmenbedingen etc. und verbessert damit insgesamt die digitale Souveränität.

Für Dienste im Bereich SaaS ist „Multi Cloud" nicht gebräuchlich.

Gerade im Hochschulumfeld ist neben der Public Cloud auch das Modell der Community Cloud zu nennen. Cloud-Dienstleistungen nach diesem Modell stehen nur Mitgliedern zu Verfügung, bspw. die bwCloud als Plattform für IaaS in Baden-Württemberg. Rechtliche Fragestellungen können sich vereinfachen, wenn die Community z.B. auf ein gemeinsames Bundesland beschränkt ist; Souveränitätsfragen können durch die Ausgestaltung der Beteiligung und Mitsprache der Teilnehmer anders gestaltet werden, als dies bei öffentlichen Angeboten möglich wäre.

5.3. DFN-Cloud-Leistungen

Nutzung der DFN-Cloud
Die Dienste des Vereins zur Förderung eines Deutschen Forschungsnetzes e.V. (DFN-Verein) sind vielfältig und unter unterschiedlichen Gesichtspunkten klassifizierbar. Neben den infrastrukturellen Basisdiensten (z.B. DFNInternet, eduroam, DFN-AAI) sind für die Betrachtung im Kontext der Cloud-Nutzung vor allem die Möglichkeiten der kollaborativen Dienste zu nennen. Dieses Dienstportfolio lässt sich anhand der unterschiedlichen Fertigungstiefen klassifizieren in

- Dienste, die vom DFN-Verein betrieben werden und
- Dienste, die vom DFN-Verein organisiert werden.

Innerhalb der Kategorie der vom DFN-Verein organisierten Dienste gibt es im Rahmen der föderierten Cloud-Dienste (oder Community Clouds) Angebote wissenschaftlicher Einrichtungen, die über Forschungspartnerschaften zustande kommen, und kommerzielle Angebote gewerblicher Anbieter (externe Cloud-Dienste), die über Vergabeverfahren von Rahmenverträgen organisiert werden. Eine Kernaufgabe für den DFN-Verein ist die Begleitung der Einrichtungen und die Vermittlung der entsprechenden Leistungen. Dabei ist die Prüfung der Nutzungsberechtigung zur Teilnahme am Wissenschaftsnetz entsprechend der Satzung des DFN-Vereins ein wichtiger Prozessbaustein.

Aktuell werden Dienste aus drei verschiedenen Kategorien angeboten:

1) **DFN-eigene Dienste:** Sie werden auf DFN-Servern On-Premises betrieben und vom DFN-Verein administriert (z.B. DFNconf, DFN-Terminplaner) oder durch beauftragte Dienstleister erbracht (z.B. DFNFernsprechen). Hier liegt ein besonderes Augenmerk auf den Anforderungen an die Datenhoheit über den gesamten Datenlebenszyklus, vom Erstellen bis zum Löschen.

2) **Föderierte Dienste:** Seit geraumer Zeit kooperiert das DFN mit Cloud-Anbietern des öffentlichen Sektors, meist aus dem Umfeld von Universitäten und Forschungseinrichtungen – es wird hier von „Föderierten Cloud-Angeboten" gesprochen. Aus Sicht des DFN sind das Community Clouds nach dem Motto „von am Wissenschaftsnetz teilnehmenden Einrichtungen für teilnehmende Einrichtungen".

3) **Rahmenverträge für gewerbliche Cloud-Dienste:** Sowohl der DFN-Verein als auch die europäische Dach organisation GÉANT haben Rahmenverträge für kommerzielle Cloud-Dienste organisiert. Unter dem Stichwort „IaaS+" sind neben grundlegenden „Infrastructure as a service"-Angeboten auch vielfältige Dateninfrastrukturen, Plattformen und Dienste erreichbar – von Spezialanwendungen für Künstliche Intelligenz und Maschinelles Lernen über Container-Entwicklungsumgebungen bis hin zu Erdbeobach tungsdiensten.Im „Software as a Service"-Bereich können DFN-Teilnehmer auf Rahmenverträge für unterschiedliche Cloud-basierte Web- und Videokonferenzdienste zugreifen. Dafür hat der DFN-Verein mit unterschiedlichen gewerblichen Anbietern Rahmenverträge abgeschlossen.

Informationsaustausch über das DFN
Das DFN erhält von den Cloud Service Providern regelmäßig Angebote für Informationsveranstaltungen, Trainings und Workshops. Ist das DFN mit Wortbeiträgen in Provider Workshops eingebunden, wird in der Regel im Newsbereich des DFN-Webauftritts und im DFN-Newsletter darüber informiert. Um ganz sicher auf dem Laufenden zu bleiben, ist das Abonnement der Cloud-Mailingliste ratsam. Für die Cloud-Videodienste besteht ebenfalls ein spezifisches Mailingangebot, weil dort mitunter ganz andere Themen von Relevanz sind. Die Listen werden vom DFN moderiert, sodass unerwünschte Werbebotschaften weitestgehend ausgeschlossen werden können.

- Als zentrales Austauschformat hat das DFN seit einiger Zeit ein sogenanntes Cloud-Forum im Rahmen der zweimal im Jahr veranstalteten DFN-Betriebstagungen etabliert. Das Forum wird von einem Sprecher oder einer Sprecherin aus der Cloud Community betreut und bietet genug Zeit für drei bis vier Vorträge

und deren Diskussion. Ein Vortragsslot ist in der Regel für das DFN vorgesehen und wird vor allem für die Präsentation von Nutzungsberichten und für aktuelle Themen genutzt. Die DFN-Betriebstagungen finden üblicherweise im März und im Oktober in Berlin statt.

- Ergänzt wird dieses Angebot durch zusätzliche Webinar-Tage, in denen unterschiedliche Vorträge präsentiert werden. Dabei sollen zu gleichen Anteilen Vorträge aus dem Bereich der föderierten Cloud, aus dem Bereich der kommerziellen Angebote und aus dem Bereich der internationalen Zusammenarbeit organisiert werden. Die Webinar-Tage werden jeweils im Vorfeld der Betriebstagungen veranstaltet und bieten so die Möglichkeit, bereits vor der jeweiligen Betriebstagung zu spezifischen Fragen ins Gespräch zu kommen.

- Bezüglich der DFN-eigenen Dienste haben sich im Rahmen der Betriebstagung ebenfalls dedizierte Foren etabliert:

  - Forum Multimedia
  - Forum Fernsprechen

Bei der zeitlichen Planung wird darauf geachtet, dass sich die Foren nicht überschneiden.

- Für die DFN-eigenen Videokonferenzdienste und die Cloud-Videodienste spielt der sogenannte VCC-Workshop des Kompetenzzentrums für Videokonferenzdienste an der TU Dresden eine wichtige Rolle. Dieser findet einmal im Jahr statt und richtet sich an administrativ-operative Nutzergruppen.
- In anlassbezogenen Workshops werden aktuelle Themen mit besonderem Augenmerk auf die Ein beziehung der nutzenden Einrichtungen gelegt. Dies kann im Vorfeld von größeren Ausschreibungen sein – bspw. OCRE – oder zu aktuellen Themen, wie Fragen zum Qualitätsmanagement im Zusammenhang mit Cloud-Diensten oder krisenhaften, die Dienstkontinuität beeinträchtigenden Situationen. Die anlassbezogenen Workshops erreichen einen hohen Grad an Partizipation und eröffnen weitreichende Mitwirkungsmöglichkeiten für die teilnehmenden Einrichtungen und werden in Formaten wie Unkonferenz, Open Space oder World Café angeboten. Die anlassbezogenen Workshops dienen auch dazu, bestehende Cloud-Angebote weiterzuentwickeln und neue Dienste zu entdecken.

Kommunikationswege
Eine zentrale strategische Herausforderung ist es für das DFN, die richtigen Kanäle für die Kommunikation mit den teilnehmenden Einrichtungen zu identifizieren. Genutzt werden folgende Informationswege:

- Begleitung der Einrichtungen
  - Gremien und Foren
  - Workshops
  - Tagungen und Kongresse
  - Arbeitskreise und Kommissionen
  - Messebesuche
  - DFN-Mitteilungen
  - DFN-Newsletter
  - Kompetenzzentrum für Videokonferenzdienste (VCC)
  - Internationale Vernetzung über GÉANT

- Koordination der Rahmenvertragspartner

  - Info-Veranstaltungen unter Beteiligung der Lieferanten
  - Betreuung und Moderation von Mailinglisten

Neben den eigenen Angeboten des DFN haben die ZKI-Arbeitskreise, die Workshops der Arbeitsgemeinschaft der Medieneinrichtungen an Hochschulen (amh) und auch die DINI-Angebote besondere Bedeutung für die DFN-Cloud. Ebenso dienen die Frühjahrs- und die Herbsttagung des ZKI zum Informationsaustausch und zur Vernetzung.

Kontinuierliche Marktanalyse
Das DFN orientiert sich bei seinen Marktbeobachtungen im Bereich von Cloud-Angeboten an den klassischen Marketingkriterien, um seinen teilnehmenden Einrichtungen zweckmäßige Cloud-Dienste anbieten zu können. Für eine multiperspektivische Sichtweise werden dazu folgende Leitfragen betrachtet:

- Wie sehen die Anforderung der teilnehmenden Einrichtungen aus?
- Welche Angebote der Lieferanten stehen dem gegenüber?
- Welche neuen Dienste zeichnen sich ab, die es zuvor noch nicht gab?
- Zeichnen sich Alternativen zu bestehenden Diensten ab?

Der Beantwortung dieser Fragen liegt ein Lebenszyklusmodell zugrunde, dass von unterschiedlichen Stadien hinsichtlich des erwarteten Marktwachstums und relativer Marktanteile einzelner Dienste ausgeht. Entsprechend passt das DFN seine Maßnahmen zur Unterstützung von Vertriebsmaßnahmen dynamisch an.

Verweise

Bundesamt für Sicherheit in der Informationstechnik (2023). IT-Grundschutz-Komp endium – Werkzeug für Informationssicherheit. Bundesamt für Sicherheit in der Informationstechnik (2023). https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html.

SDM (2022). Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz). https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode-V30a.pdf.

Wissenschaftsrat (2023). Empfehlungen zur Souveränität und Sicherheit der Wissenschaft im digitalen Raum. Köln. https://doi:10.57674/m6pk-dt95.

ZKI (2021). Ergebnisbericht ZKI-Kommission Cloud. https://doi.org/10.5281/zenodo.5702566.
ZKI (2022). Sicherstellung der digitalen Souveränität und Bildungsgerechtigkeit – Empfehlungen zur Ausgestaltung von Rahmenbedingungen für die Nutzung von Cloud-basierten Angeboten im Bildungsbereich. https://doi.org/10.5281/zenodo.7104141.

Zentren für
Kommunikation und
Informationsverarbeitung e.V.

Erfahren Sie mehr:

www.zki.de

events.zki.de