



CIO-Positionspapier Digitale Souveränität an Universitäten und Hochschulen



28.03.2025

Einführung

Die Zielsetzung des Positionspapiers besteht darin, aus Sicht von Chief Information Officers (CIOs)¹ von Universitäten und Hochschulen² die Bedeutung der digitalen Souveränität an Universitäten und Hochschulen herauszustellen, konkrete Handlungsempfehlungen zur Stärkung der digitalen Souveränität abzuleiten und ausgewählte Aufgabenbereiche näher zu definieren.

2023 hat der Wissenschaftsrat in seinen Empfehlungen zur „Souveränität und Sicherheit der Wissenschaft im digitalen Raum“ (Wissenschaftsrat [2023](#)) auf die Bedeutung des Themas hingewiesen. Unser Positionspapier geht auf diese Empfehlungen ein und diskutiert diese aus der Perspektive der CIOs, also derjenigen, die an den Universitäten und Hochschulen im Bereich der IT tätig sind. Das Positionspapier wurde gemeinschaftlich von CIOs der Universitäten in Baden-Württemberg und Universitäten und Hochschulen in Bayern erarbeitet.

Digitale Souveränität ist eine essenzielle Grundlage für vertrauenswürdige IT-Lösungen und eine unverzichtbare Voraussetzung für unabhängiges Handeln. Digital souveräne Universitäten und Hochschulen zeichnen sich durch geringe Abhängigkeiten z. B. gegenüber Herstellern und Dienstleistern von IT-Technologie aus und bewahren sich größere Gestaltungsspielräume. Damit ist die digitale Souveränität aus unserer Sicht ein Gestaltungs- und Sicherheitsthema für die Hochschulleitungen und sollte aktiv von den CIOs der Universitäten und Hochschulen angegangen werden.

Entsprechend ist es unser Anliegen, die digitale Selbstbestimmung in allen Bereichen (Forschung, Studium und Lehre sowie in den wissenschaftsunterstützenden Bereichen) auf der obersten Entscheidungsebene anzusiedeln. Von dieser Position aus kann auch die Vernetzung nach innen und nach außen gelingen. In diesem Papier wird die Bedeutung der digitalen Souveränität für Universitäten und Hochschulen sowie deren Chancen und Grenzen anhand von Fallbeispielen verdeutlicht.

¹ Das Positionspapier wurde von einer gemeinsamen Arbeitsgruppe der CIOs der Universitäten in Baden-Württemberg sowie der CIOs der Universitäten und Hochschulen für angewandte Wissenschaft (HAWs) in Bayern verfasst.

² Wir danken den Vertretungen der universitären Rechenzentren in Baden-Württemberg für die konstruktive Diskussion des Positionspapiers.

Die fortschreitende Digitalisierung der Universitäten und Hochschulen bietet Chancen zur Stärkung der digitalen Souveränität, erfordert jedoch auch eine aktive Steuerung und den Schutz vor Risiken. Gleichzeitig ergibt sich eine Vielzahl an neuen Herausforderungen (Rechnungshof Baden-Württemberg [2022](#)). Dabei unterstützen umfassende Konzepte (BMWi [2021](#), IT-Planungsrat [2021](#), Sachverständigenrat für Verbraucherfragen [2017](#)) u.a. zum Schutz personenbezogener Daten, zur Gewährleistung der digitalen Grundrechte wie Meinungsfreiheit oder Privatsphäre sowie zur Kontrolle über die digitale Infrastruktur und Dienste. Die Art und Weise, wie diese Herausforderungen bewältigt werden, kann dazu beitragen, die digitale Souveränität zu bewahren oder zu mindern.

Universitäten und Hochschulen spielen eine wichtige Rolle bei der Förderung der digitalen Souveränität, da sie einerseits im Rahmen ihrer Forschungstätigkeiten innovative Lösungen entwickeln, die zur digitalen Souveränität beitragen können, andererseits im Rahmen der Lehrtätigkeit in vielen Fachdisziplinen entsprechende Kompetenzen vermitteln und dadurch das Bewusstsein für die Bedeutung der digitalen Souveränität schärfen. Der Blick wird auch auf die Weiterentwicklung der IT-Infrastruktur gerichtet, denn dadurch leisten die Universitäten und Hochschulen einen weiteren Beitrag zur Sicherung und Förderung der digitalen Souveränität. Allerdings kann ein hoher Grad an digitaler Souveränität mit erheblichen Kosten verbunden sein. Diese personellen und finanziellen Aufwände entstehen durch den Aufbau und die Pflege von notwendigen alternativen, eigenen IT-Infrastrukturen, welche den Anforderungen der digitalen Souveränität gerecht werden.

Der Betrieb und vor allem die Weiterentwicklung der IT an den Universitäten und Hochschulen steht folglich im Spannungsfeld mit anderen strategischen Fragen. Die Beurteilung von Abhängigkeiten im digitalen Raum bildet somit zusammen mit den zu berücksichtigenden Faktoren als Grundlage zur Ausgestaltung der digitalen Souveränität einen Schwerpunkt des Positionspapiers.

Begriffliche Abgrenzung: digitale Souveränität an Universitäten und Hochschulen

Der Begriff der digitalen Souveränität ist vielschichtig und komplex, da er in unterschiedlichen Kontexten (Recht, Politik, Wirtschaft, Gesellschaft) oder für unterschiedliche gesellschaftliche Rollen (Personal, Privatperson, Institution) sowie aus einer wirtschaftlichen oder gesamtgesellschaftlichen Sicht betrachtet werden kann. Mit digitaler Souveränität verbunden wird die Unabhängigkeit, Eigenverantwortlichkeit und Selbstbestimmtheit von Akteuren in der digitalen Welt. Nur vereinzelt werden konkrete Kategorien, anhand derer die digitale Souveränität bzw. das Ausmaß der Abhängigkeit im digitalen Raum bestimmt werden kann, dargelegt (z. B. BMWK [2018](#), Bacharach, Jäger, Wehnes [2023](#)).

Im Rahmen dieses Positionspapiers verstehen wir digitale Souveränität als „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbständig, selbstbestimmt und sicher ausüben zu können“ (ÖFIT [2017](#)). Für Universitäten und Hochschulen bezieht sich die digitale Souveränität auf die Fähigkeiten (1) in der digitalen Welt unabhängig zu handeln, (2) die Kontrolle über ihre digitalen Angelegenheiten in Forschung, Lehre und im wissenschaftsunterstützenden Bereich zu behalten und (3) ihre Daten sowie digitale Infrastruktur unter ihrer eigenen Hoheit zu haben. Dies umfasst auch digitale Techniken und Dienste nach eigenen Regeln und Standards zu entwickeln, zu nutzen und zu schützen, ohne von Externen wie z. B. IT-Anbietern oder Softwareherstellern abhängig zu sein oder zu werden (IT-Planungsrat [2021](#)). So zeigte 2024 die Kündigung des Vertrags zur Zertifikatherstellung durch einen zentralen externen Dienstleister

für den ganzen europäischen Wissenschaftsbereich konkret die Gefahren einer fehlenden digitalen Souveränität.

Entscheidungsdimensionen zur Abwägung der digitalen Souveränität an Universitäten und Hochschulen

Das Leitprinzip einer digitalen Souveränität zeigt sich in allen Aufgabenbereichen einer Universität oder Hochschule:

- In der Forschung: Um den Anforderungen von Forschenden an ein kollaboratives Arbeiten gerecht zu werden, werden zunehmend Forschungsdaten in die Ökosysteme großer Cloud-Anbieter verschoben, was Abhängigkeiten erzeugt und die Verfügungsmöglichkeiten einschränkt (Wissenschaftsrat [2023](#)).
- In Studium und Lehre: Angetrieben durch die COVID 19-Pandemie stieg der Bedarf an digitalen Lern- und Lehrformaten und damit auch die Abhängigkeit von bestimmten Lösungen wie Videokonferenzsystemen oder Lernmanagement-Plattformen.
- Im wissenschaftsunterstützenden Bereich: Mit der Digitalisierung der Unterstützungsstrukturen an Universitäten und Hochschulen entstehen im Verwaltungsbereich zunehmende Verschränkung von Geschäftsprozessen mit digitalen Workflow-Lösungen und Datenhaltungssystemen.

Die verschiedenen Aufgabenbereiche an Universitäten und Hochschulen verdeutlichen, dass eine vollständige digitale Souveränität kaum realistisch ist, sondern nur in Ansätzen erreicht werden kann (Arbeitsgruppe „Digitale Souveränität“ [2024](#)). Dennoch sollte digitale Souveränität angestrebt werden, da sonst die Gefahr von sogenannten *Lock-in-Effekten* durch eine zunehmende Bindung an kommerzielle Anbieter droht. Ein hoher Grad an digitaler Souveränität ist jedoch zumeist mit hohem personellem und finanziellem Aufwand verbunden. Gleichzeitig spielen andere Faktoren wie Funktionalität, Usability und die Skalierbarkeit von digitalen Lösungen eine wichtige Rolle. Bei der Entwicklung einer Cloud-Strategie sind beispielsweise Anforderungen an den Cloud-Provider und an die Sicherheit und Leistungsfähigkeit der Cloud-Infrastruktur ebenfalls wichtige Faktoren. Letztlich ergibt sich daraus ein Spannungsfeld zwischen verschiedenen übergeordneten Entscheidungsdimensionen (z. B. Wirtschaftlichkeit) und darin abgebildeten Kriterien, welche es aufzulösen gilt. Darüber hinaus ist zu bedenken, dass Lock-in-Effekte nicht nur im Zusammenhang mit der Nutzung von kommerzieller Software auftreten können, sondern auch wenn man die Strategie verfolgt, eigene IT-Infrastruktur aufzubauen, welche den Anforderungen der digitalen Souveränität gerecht wird. Durch eine unzureichende IT-Personalausstattung kann es zu Know-how-Monopolen bei Mitarbeitenden kommen. Diese Abhängigkeit von personellen Ressourcen kann ein Risiko für die Organisationskontinuität bei Ausfall oder Kündigung der Mitarbeitenden darstellen.

Für den Betrieb und die Weiterentwicklung der IT an den Universitäten und Hochschulen ist folglich nicht allein die Sicherung digitaler Souveränität entscheidend, sondern es sind weitere Faktoren zu berücksichtigen. Diese beziehen sich vor allem auf (1) technische Rahmenbedingungen (z. B. Skalierbarkeit der IT-Systeme), die die Ausgangssituation festlegen, (2) die eigenen strategischen Ziele und abgeleiteten Priorisierungen und auf (3) die generell mit der Weiterentwicklung verbundenen Kosten und Aufwendungen. Der angestrebte Grad an digitaler Souveränität sollte entsprechend einer Entscheidung unterliegen, in der die unterschiedlichen strategischen Faktoren sorgfältig abgewogen werden müssen.

Folgende Entscheidungsdimensionen zur digitalen Souveränität sind zu berücksichtigen:

I. Datenschutz und Cybersicherheit

An Universitäten und Hochschulen werden große Mengen an sensiblen Daten in den Bereichen Forschung (z. B. streng vertrauliche Forschungsprojekte), Lehre (z. B. Daten von Studierenden) und in den wissenschaftsunterstützenden Bereichen (z. B. Daten von Mitarbeitenden) verarbeitet. Es gilt, diese vor unbefugtem Zugriff zu schützen und die Hoheit über die Daten zu behalten. Datenschutzverletzungen können nicht nur zu rechtlichen Konsequenzen führen, sondern auch das Vertrauen der Öffentlichkeit und v.a. der Studierenden in die jeweilige Universität oder Hochschule nachhaltig beeinträchtigen. Gleichzeitig ist das Risiko von Cyberangriffen erhöht und forciert den Aufbau von Kapazitäten zur Gewährleistung der notwendigen IT-Sicherheit. Dies umfasst u.a. die Umsetzung von robusten Datenschutzmaßnahmen, Sensibilisierung der Mitarbeitenden, Nutzung von Verschlüsselungstechnologien, Durchführung von regelmäßigen Schwachstellenscans, Erstellung von Sicherheitsrichtlinien und den Aufbau einer entsprechenden Notfallinfrastruktur (z. B. CSIRT).

II. Grad der Unabhängigkeit

Insbesondere für Universitäten und Hochschulen ist es eine Frage der Risikoabwägung, die Hoheit über die eigenen Daten zu behalten. Bei eingesetzten IT-Lösungen ist der Grad der notwendigen und akzeptierten Abhängigkeit zu definieren. Dabei ist die potenzielle Reversibilität von Entscheidungen zu bedenken. So sollte eine *Exit-Strategie* die Möglichkeit berücksichtigen, dass die wichtigsten *Assets* wie Daten zurückgeholt werden können.

Zur digitalen Verarbeitung von Daten und Unterstützung von Prozessen in Universitäten und Hochschulen werden vielfältige Softwareprodukte und Dienste eingesetzt, die aus unterschiedlichen Quellen von Open Source bis zu externen IT-Anbietern reichen. Die Verwendung von Open Source-Software und -Technologien kann dazu beitragen, die Abhängigkeit von proprietären Lösungen zu verringern und die Kontrolle über die eigenen IT-Ressourcen zu erhöhen, da Quellcodes überprüft, angepasst und unabhängig von einzelnen Anbietern weiterentwickelt werden können. Die Nutzung und Integration von Quellcode durch die Universität oder Hochschule kann durch verschiedene Lizenztypen definiert sein: Proprietary Licence, Copyleft Licence, Permissive Licence oder Public-domain lizenzierter Quelle (ugs. Open Source). Nur letzterer ist öffentlich verfügbar und kann von der Universität bzw. Hochschule frei verwendet und verändert werden.

Kommerzielle Angebote können nach Risikoabschätzung eine akzeptable Alternative sein. An Kernbereiche, die als essenziell für Universitäten und Hochschulen mit unbedingter Unabhängigkeit definiert wurden, sind höhere Anforderungen an eingesetzte IT-Lösungen zu stellen. Generell ist stets der Überblick über aktuelle Wahlmöglichkeiten zu behalten (Unternehmens- oder Open Source-Alternativen). Diese Betrachtung gilt auch für den Einsatz von Technologien der generativen Künstlichen Intelligenz, die sowohl in den verwendeten Sprachmodellen (LLM) wie auch bei den Trainingsdaten je nach Anbieter unterschiedlich proprietär oder offengelegt sind.

III. Wirtschaftlichkeit

Bei der Auswahl von IT-Lösungen sind die Wirtschaftlichkeit, Anpassungsfähigkeit und der Ressourceneinsatz von hoher Relevanz, insbesondere bei knappem IT-Personal und hohem Digitalisierungsdruck. Bei der Bewertung von Softwareprodukten und -diensten sind Begleitkosten

(wie z. B. Lizenzmanagement, Anpassungsaufwände, Schulungsaufwände, Personal und Hardware, Beratungsleistungen) zu berücksichtigen. Dies beeinflusst ebenfalls die Entscheidung über *Make-or-Buy*. Durch Zentralisierung von Standardleistungen (z. B. über einen Verbund) werden durch Skaleneffekte Kosteneinsparungen realisiert und die eingesetzten IT-Lösungen besser überblickt. Übergreifende Kooperationen und Abstimmungen bringen die Partner auch in eine bessere Verhandlungsposition gegenüber Anbietern und erlauben so einrichtungsübergreifende Dual-Vendor-Strategien. Es ist auch zu hinterfragen, ob die Anpassung und Modernisierung lokaler Prozesse eine höhere Wertschöpfung des Softwareeinsatzes ermöglicht.

Es dürfen dabei nicht nur die aktuellen Kosten berücksichtigt werden, sondern es muss von Beginn an mit eingeplant werden, wie sich mögliche Lock-In-Effekte (vgl. M365, Adobe) auf die langfristige Preisgestaltung auswirken können und welche Kosten mit einem später Anbieterwechsel (*Exit-Strategie*) einhergehen. Dies gilt für Vendor-Lock-In-Situationen ebenso wie für Lock-In aufgrund spezialisierter Kenntnisse von Mitarbeitenden oder fehlender Finanzierung. Unter Umständen können durch abgestimmtes Vorgehen mittels Verträgen mit Dritten gewisse negative Effekte mitigiert werden, was frühzeitig zu planen und entsprechend rechtlich zu begleiten ist.

IV. Nutzerfreundlichkeit

Die eingesetzten Dienste an Hochschulen verfügen oftmals über eine breite Nutzerbasis von Dozierenden über Verwaltungsmitarbeitende bis hin zu Studierenden. Aufgrund dieser heterogenen Nutzergruppen ist es umso wichtiger, dass die eingesetzten Dienste eine hohe Benutzerfreundlichkeit aufweisen, damit selbstständig, schnell sowie unkompliziert damit umgegangen werden kann. Ein intuitives Design vermindert den Einarbeitungsaufwand und reduziert dadurch den notwendigen Bedarf an Schulungen und Unterstützungsstrukturen. Übersichtliche Benutzeroberflächen ermöglichen es Nutzenden zudem Aufgaben schneller zu erledigen, was zu Effizienzsteigerungen führen kann. Unabhängig davon, müssen die Dienste zuverlässig, sicher sowie reibungsfrei erbracht werden und eine hohe Verfügbarkeit aufweisen. Bei der Auswahl von IT-Lösungen sind daher die Usability, das Handling und die Verfügbarkeit als Schlüsselfaktoren zu berücksichtigen, um so die notwendige Akzeptanz für eine breite Nutzung der Dienste zu schaffen.

V. Nachhaltigkeit

Nachhaltigkeit bezieht sich auf die Fähigkeit, die Bedürfnisse der heutigen Generation zu erfüllen, ohne die Möglichkeit zukünftiger Generationen zu beeinträchtigen, ihre eigenen Bedürfnisse zu erfüllen. Es werden ökologische, ökonomische und soziale Dimensionen unterschieden. Im Kontext der Digitalisierung bedeutet Nachhaltigkeit, Ressourcen effizient zu nutzen, Umweltbelastungen zu minimieren und auf eine langfristige Perspektive hin zu planen. Dies ist auch im Zusammenhang mit der Nachhaltigkeitsberichtserstattung von Universitäten und Hochschulen relevant. Eine nachhaltige Nutzung digitaler Technologien trägt dazu bei, Ressourcen zu schonen und Umweltbelastungen zu reduzieren. Gleichzeitig geht es darum sicherzustellen, dass die Nutzung digitaler Technologien im Einklang mit den Werten und Interessen einer Gesellschaft erfolgt. Ebenso fungieren gesetzliche Vorgaben zunehmend als Treiber der Nachhaltigkeit (z. B. Erneuerbare-Energien-Gesetz 2023), welche zumindest zum Teil auch Universitäten und Hochschulen betreffen und somit einzuhalten sind.

Fallbeispiele

Für die digitale Souveränität an Universitäten und Hochschulen und die Auseinandersetzung mit den betreffenden Entscheidungsdimensionen lassen sich konkrete Fallbeispiele aus den Bereichen Forschung, Studium und Lehre sowie aus den wissenschaftsunterstützenden Bereichen nennen.

bwHPC

Für die effiziente und autonome Versorgung der Wissenschaft in Baden-Württemberg haben die neun Landesuniversitäten ab 2012 das gemeinsame Rahmenkonzept bwHPC entwickelt, ein abgestimmtes Konzept für das High Performance Computing (HPC), das inzwischen mehrfach positiv durch die DFG begutachtet wurde.³ Zentraler Bestandteil des Konzeptes ist die Aufteilung der HPC-Komponenten auf Tier-3 auf ein Universalcluster am KIT und vier dedizierte Forschungscluster (Freiburg, Heidelberg, Tübingen und Ulm), die jeweils landesweit speziellen Forschungsgebieten auf Basis der DFG-Fachsystematik zugewiesen sind. Durch diese besondere Form der Kollaboration konnten auf die Bedürfnisse der jeweiligen Fächer angepasste Supportstrukturen in Kompetenzzentren und Tiger Teams aufgebaut werden. Insgesamt versorgt diese Kooperationsstruktur die Wissenschaft des Landes Baden-Württemberg mit einer leistungsfähigen HPC-Infrastruktur und sichert zentral die digitale Souveränität der Daten. Zum Zeitpunkt der Einführung des Konzepts gab es keine wirtschaftlich vertretbaren Alternativen, die das notwendige Niveau der Wissenschaft abdecken konnten.

Entscheidungsgrundlage

- Datenschutz und Cybersicherheit: Zentrale Abwehr ist besser als verteilte Last auf ohnehin beanspruchtes Personal vor Ort.
- Grad der Unabhängigkeit: Universitäten und Hochschulen müssen sich auf zentrale Dienste und Beschaffungen einigen, funktioniert durch Absprachen innerhalb der Forschungsgebiete.
- Wirtschaftlichkeit: Gemeinsame Fixkosten können besser aufgeteilt werden, was auch für den Geldgeber (in diesem Fall das Ministerium) wirtschaftlich ist; durch Fokussierung der Fächergruppen auf spezielle Cluster ergeben sich Effizienzgewinne bei Support und Betrieb.
- Nutzerfreundlichkeit: Forschungsgebiete bekommen eigene angepasste Supportstrukturen, besser als *nur technischer* Support in der einzelnen Universität und Hochschule.
- Nachhaltigkeit: Gemeinsame Beschaffung vermindert energieineffiziente lokale Einzelsysteme, landesweite Absprache zur Dimensionierung der Rechenleistung verringert Energiebedarf.

Campusmanagementsystem HIS eG

Zu den Kernaufgaben einer Hochschule gehören Studium und Lehre, ein Bereich, der vom Bewerbungs- und Auswahlprozess über Immatrikulation, Studierendenverwaltung, Verwaltungen von Lehrveranstaltungen und Prüfungen bis hin zu Alumni besondere Anforderungen an die Administration stellt.

1969 hat die Volkswagenstiftung in Hannover das Softwarehaus Hochschul-Informationssystem (HIS) gegründet, das 1974 in Trägerschaft von Bund und Länder übergang. Aufgabe dieses Softwarehauses ist es, die speziellen Anforderungen des Hochschulbereichs an den sogenannten Student Lifecycle Process in einer Software abzubilden. Um die Versorgung mit der für die Universitäten und Hochschulen unverzichtbaren speziellen Software und damit verbundenen Dienstleistungen zu

³ Siehe Leiter der Rechen- bzw. Informationszentren der Universitäten des Landes Baden-Württemberg (2012) und Leiterinnen und Leiter der Rechenzentren bzw. Informationszentren der Universitäten des Landes Baden-Württemberg (2019).

gewährleisten, haben 2014 die Universität und Hochschulen selbst die Trägerschaft und Verantwortung für HIS in Form einer eingetragenen Genossenschaft (eG) übernommen. Seither steuern sie in Eigenverantwortung ihr Softwarehaus. In dieser Zeit wurde die Zahl der Beschäftigten etwa verdoppelt, und es wurden neue, auf die Bedürfnisse der Universitäten und Hochschulen angepasste Produktbereiche, wie das Forschungsmanagement und die Verwaltung von Promovierenden, entwickelt und den Universitäten und Hochschulen bereitgestellt. Den Universitäten und Hochschulen stehen durch die von ihnen gesteuerte HIS eG damit eine stabile, unabhängige Versorgung in diesem speziellen geschäftskritischen Bereich zur Verfügung, der im Rahmen der fortschreitenden Digitalisierung täglich an Bedeutung gewinnt.

Entscheidungsgrundlage

- **Datenschutz und Cybersicherheit:** Stabile Lösung wird geteilt an vielen Universitäten und Hochschulen, zentral behobene Sicherheitsprobleme führen zu einem Schutz für alle im Falle eines lokalen Angriffs.
- **Grad der Unabhängigkeit:** Dienste sind speziell zugeschnitten auf Bedarf von Universitäten und Hochschulen vs. Vendor-Lock-in-Risikoabwägung.
- **Wirtschaftlichkeit:** Gemeinsame Fixkosten können besser geteilt werden, demokratische Genossenschaftslösung, Synergiesteigerung durch gemeinsame Planung und Entwicklung.
- **Nutzerfreundlichkeit:** Weiterentwicklung der Software in enger Absprache mit Nutzenden.
- **Nachhaltigkeit:** Alle erwirtschafteten Gewinne fließen ausschließlich in die gesetzliche Rücklage und kommen allen Genossenschaftsmitgliedern zugute.

Bibliothekssystem FOLIO

Im für die Hochschulwelt wichtigen Bereich der lokalen Bibliothekssysteme für wissenschaftliche Bibliotheken bestehen weltweit im Wesentlichen zwei kommerzielle Angebote, welche direkt mit der Datenhaltung in einer externen Cloud verbunden sind. Mit FOLIO entsteht momentan eine Open Source Alternative, welche neben der freien Software auch die Datenhaltung und den Betrieb on-premises erlaubt und damit die Souveränität der wissenschaftlichen Bibliotheken stützt.

In Deutschland haben sich bereits mehrere Bibliotheksverbände für FOLIO entschieden, ebenso entstehen Betriebszentren für die kollaborative Versorgung der wissenschaftlichen Bibliotheken am Gemeinsamen Bibliotheksverbund (GBV) in Göttingen, dem Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften in München und dem Zentrum für Datenverarbeitung in Tübingen. Die bayerischen Universitäten und Hochschulen haben sich für die landesweite Einführung von FOLIO bereits entschieden, in Baden-Württemberg wird in einem vom Wissenschaftsministerium geförderten Projekt bwFOLIO der mögliche Einsatz von FOLIO evaluiert und vorbereitet. Der GBV hat sich ebenfalls für die Einführung von FOLIO entschieden und ist mit dem ERM-Modul von Folio aktuell 24 Bibliotheken bereits im Produktivbetrieb.

Entscheidungsgrundlage

- **Datenschutz und Cybersicherheit:** Stabile Lösung, die geteilt verwaltet werden kann.
- **Grad der Unabhängigkeit:** Dienste können spezifisch für Uni-Bibliotheken entwickelt werden, Passgenauigkeit des Angebotes, Risikoabwägung Vendor-Lock-In wg. externer Cloud.
- **Wirtschaftlichkeit:** Open Source Lösung ermöglicht geringe Fixkosten, kein Lizenzkosten-Lock-In (externe Cloud).

- Nutzerfreundlichkeit: Weiterentwicklung der Software gelingt in enger Absprache mit Nutzenden in den Bibliotheken.
- Nachhaltigkeit: Betrieb erfolgt on-premises.

HITS-Beschaffung

Die IT-Rahmenverträge sind – insbesondere durch ihre Abbildung auf elektronischen Beschaffungsportalen (eProcurement) – eine grundlegende Basis für alle IT-Prozesse an den bayerischen Universitäten und Hochschulen. Gleichzeitig sind sie ein wesentlicher Beitrag zur Erfüllung der zunehmenden Anforderungen an Compliance und Governance-Management. Ohne dieses Fundament sind die IT-Dienstleistungen nicht mehr effizient und bedarfsgerecht zu erfüllen. Auf Grund des erheblichen Umfangs können die bayerischen Universitäten und Hochschulen dieses komplexe Aufgabengebiet nur in enger Kooperation und mittels gemeinsam genutzter Dienste erfüllen. Die Kooperationen zwischen den bayerischen Universitäten und Hochschulen waren ursprünglich vorrangig zur Verringerung des mit Ausschreibungen verbundenen Aufwands entstanden. Mittlerweile legen die Rahmenverträge den Grundstein für den gesamten Beschaffungsprozess, bestehend aus den klassischen Bausteinen:

- Rahmenvertrag (Festlegung der Rahmenbedingungen, Ausschreibung, Vertragsverhandlungen und Vertragsschluss, eVergabe),
- Beschaffungsvorgang (eProcurement, Auftrag, Rechnungsstellung, Buchung, Inventarisierung) und
- Deployment (Konfiguration, Inbetriebnahme, Installation, Provisionierung) sowie
- spätere Nutzung und Betreuung (Garantieabwicklung, Support).

Diese Beschaffungsprozesse werden in einem hochschultypübergreifenden Hochschulzentrum (HITS) des Digitalverbunds Bayern bearbeitet, das sich verantwortungsmäßig über mehrere bayerischen Universitäten und Hochschulen erstreckt. Die Koordinierung und Abwicklung gemeinsamer IT-Rahmenverträge haben einen wichtigen Beitrag zur Stärkung der digitalen Souveränität und der Digitalisierung der Beschaffungsprozesse an den Universitäten und Hochschulen in Bayern geleistet. Die Definition von hochschultypübergreifenden Anforderungen an die Beschaffung durch die gemeinsamen IT-Rahmenverträge hat die Abhängigkeit von einzelnen Anbietern deutlich reduziert. Dennoch gibt es Marktbereiche, in denen nahezu eine Monopolstellung bestimmter kommerzieller Anbieter besteht und qualitativ vergleichbare Open Source-Lösungen fehlen, weshalb selbst durch hochschultypübergreifende Beschaffungen eine Reduzierung von Abhängigkeiten in solchen Fällen, zumindest kurzfristig, kaum möglich erscheint.

Entscheidungsgrundlage

- Datenschutz und Cybersicherheit: keine Auswirkung.
- Grad der Unabhängigkeit: Universitäten und Hochschulen müssen sich auf ein Portfolio an Soft- und Hardware und gemeinsamen Anforderungen zu deren Beschaffung einigen. Manchmal kommt es dabei zu einer Dual-Source-Strategien (bspw. NG Firewall mit zwei Anbietern).
- Wirtschaftlichkeit: HITS-Beschaffung hat seit seiner Gründung insgesamt bereits über 90 Mio. EUR eingespart.
- Nutzerfreundlichkeit: Die Dienstleistung der Beschaffungsprozesse wird mit beteiligten Rechenzentren und den IT-Einkaufsstrukturen der Universitäten und Hochschulen weiterentwickelt. Webshop mit direkter Anbindung an die Beschaffungssoftware wurde programmiert und wird kontinuierlich weiterentwickelt.

- Nachhaltigkeit: Eine gemeinsame IT-Beschaffung kann neben den wirtschaftlichen Bedarfen aller Universitäten und Hochschulen auch ökologische und soziale Nachhaltigkeitskriterien bündeln und adressieren.

Handlungsempfehlungen

Zur Förderung der digitalen Souveränität und in Hinblick auf die Best Practice-Beispiele lassen sich folgende Empfehlungen ableiten:

I. Berücksichtigung in der Hochschulstrategie

Die Aufstellung in Bezug auf digitale Souveränität ist von großer strategischer Relevanz für Universitäten und Hochschulen. Daher sollte die digitale Souveränität in der Hochschulstrategie und den Strategie- und Entwicklungsplänen berücksichtigt werden. Im Rahmen der Strategiefindung sollte dabei die Frage nach der besten Flexibilität, Skalierbarkeit und IT-Sicherheit der IT-Infrastruktur nicht dogmatisch beantwortet werden, sondern benötigt ein Zusammenspiel von eigener IT-Infrastruktur (*on-premises* im eigenen Rechenzentrum) und externen Lösungen (Rechenzentren anderer Hochschulen, privater Unternehmen oder Cloud-Lösungen). Es ist jedoch wichtig sicherzustellen, dass sensible Daten und Dienste in der Cloud den Sicherheitsanforderungen entsprechen und die Kontrolle über die Daten erhalten bleibt.

II. Aufbau einer Governance-Struktur und interne Vernetzung

Für eine effiziente Behandlung und konsistente Entscheidungsfindung an Universitäten und Hochschulen ist eine Governance-Struktur und interne Vernetzung der verschiedenen Bereiche erforderlich. So kann sichergestellt werden, dass Entscheidungen im Einklang mit den Zielen der digitalen Souveränität getroffen werden. Die digitale Souveränität betrifft alle Bereiche der Universitäten und Hochschulen: Forschung, Studium, Lehre und die wissenschaftsunterstützenden Bereiche. Die Verantwortlichkeit sollte daher einer CIO-Funktion zugeordnet werden.

III. Hochschul(typ)übergreifende Kooperation und gemeinsame Strategieentwicklung

Eine gemeinsame Strategieentwicklung in Kooperation mit anderen Universitäten und Hochschulen unterstützt die Wahrung der digitalen Souveränität. Hochschulinterne und -übergreifende Kooperationen tragen dazu bei, Ressourcen zu bündeln, Synergien zu schöpfen und Standards gemeinsam umzusetzen und ggf. wirtschaftlicher agieren zu können. Durch den Austausch und die Vernetzung mit Partnerinstitutionen können Informationen und Erfahrungen geteilt und gemeinsame Entscheidungen und abgestimmtes Handeln gefördert werden. Hochschul(typ)übergreifende Kooperationen dienen dem Wissenstransfer und der gemeinsamen Handhabung von übergreifenden IT-Lösungen, um mit- und voneinander zu lernen und Skalenerträge zu realisieren. Sie stellen zudem eine Möglichkeit dar, sich gegenseitig *Software as a Service (SaaS)*-Dienste unabhängig von Dritten anzubieten. Auch eröffnen sich durch Kooperationen neue strategische Optionen (z. B. *Dual-Sourcing-Strategien*). Durch hochschul(typ)übergreifende IT-Serviceangebote wird ebenso der Lock-in-Effekt der IT-Ressourcen-Abhängigkeit vermindert, da derartige Serviceangebote i. d. R. durch Teams und nicht durch einzelne Mitarbeiter erbracht werden. Die Entstehung der Gefahr von Know-how-Monopolen bei einzelnen Mitarbeitenden wird damit verringert.

IV. Regelmäßige Folgenabschätzung

Die Berücksichtigung digitaler Souveränität an Universitäten und Hochschulen ist eine Daueraufgabe. Vor dem Einsatz IT-basierter Dienste sollten die Chancen und Risiken umfänglich untersucht und eine begründete Entscheidung hinsichtlich ihrer Nutzung dokumentiert getroffen werden. Wegen allfälliger

Änderungen von Software, deren Eigentumsverhältnissen und Lizenzbedingungen sind regelmäßig erneute Prüfungen notwendig, um sicherheits- und datenschutzrelevante Aspekte, Relevanz in der jeweiligen Forschungs-Community und Wirtschaftlichkeit im Blick zu behalten. Daraus sollen Maßnahmen für die Reduktion der Risiken abgeleitet und Handlungsempfehlungen für die optimale Nutzung gegeben werden.

V. Change Management

Die Einführung neuer IT-Systeme und das Revidieren von Entscheidungen zur Verbesserung der digitalen Souveränität erfordert ein kompetentes Veränderungsmanagement, um sicherzustellen, dass die Universitäts- und Hochschulangehörigen diese Veränderungen auch akzeptieren und entsprechende IT-Lösungen nutzen. Eine transparente und gezielte Kommunikation sowie Informations- und Schulungsangebote sind wichtige flankierende Maßnahmen. Beim Change Management handelt es sich vorwiegend um eine organisatorische Aufgabe – diese gehört daher nicht per se in das universitäre Rechenzentrum, sondern in die Nähe der Universitäts- bzw. Hochschulleitung, Personalentwicklung und Hochschulkommunikation.

VI. Kompetenzentwicklung

Die digitale Souveränität kann durch eine zunehmende Medienkompetenz der Nutzenden verbessert werden. *Digital Literacy* adressiert die Urteilsfähigkeit, Selbstbestimmtheit und das Verantwortungsbewusstsein der Nutzenden und führt dazu, dass die Wirkungen des eigenen Handelns erkannt und auch bewertet werden können. AI Literacy bezieht sich auf die Fähigkeit, KI-Systeme zu verstehen, kritisch zu hinterfragen und effektiv zu nutzen. Entsprechende Angebote zur Förderung für Universitäts- und Hochschulangehörige sollten ausgebaut werden, um das Verständnis für die Folgen des Umgangs mit und des Einsatzes von IT-Lösungen zu stärken. Die Kompetenzentwicklung betrifft auch die IT-Verantwortlichen der Rechenzentren, welche auch die organisatorischen Voraussetzungen und Konsequenzen von Technologieeinführungen verstehen müssen.

Ausblick

Die Förderung der digitalen Souveränität ist in den Strategie- und Planungsprozessen von Universitäten und Hochschulen zu berücksichtigen und zu verankern. Die Umsetzung erforderlicher Maßnahmen zur digitalen Souveränität benötigt entsprechende Ressourcen, die von kompetentem Personal bis hin zu einer ausreichenden Budgetierung reichen. Insofern ist die Verbesserung der Rahmenbedingungen für Personalgewinnung, Personalentwicklung und Qualifikation im IT-Bereich erfolgskritisch, um den steigenden Anforderungen in einer schon komplexen System- und Dienstelandschaft in der Universitäts- und Hochschul-IT zu begegnen.

Hierbei können auch hochschul(typ)übergreifende Kooperationen unterstützen, um gezielt knappe Ressourcen im IT-Bereich zu bündeln und Skaleneffekte zu erzielen. Ein entsprechender Schritt könnte der Aufbau eines hochschul(typ)übergreifenden Enterprise Architecture Managements (EAMs) in Verbindung mit einem Konzept zur Messung digitaler Souveränität sein, um eine Übersicht der kritischen IT-Systeme mit Bezug zu den zugehörigen Geschäftsprozessen oder Geschäftsfähigkeiten zu erhalten. Durch die entstehende Transparenz können Systeme mit einem hohen Maß an Abhängigkeit aufgedeckt und frühzeitig gemeinsam Maßnahmen zur Verbesserung der digitalen Souveränität eingeleitet werden (z. B. Dual-Sourcing-Strategie oder gemeinschaftliche Anwendungsentwicklungen), bevor negative Konsequenzen wie Lock-in-Effekte mit übermäßigen Kostensteigerungen eintreten. Die Universitäten und Hochschulen werden dadurch zu einem proaktiven und strategischen Management der digitalen Souveränität befähigt.

Einzelnachweise

- Arbeitsgruppe „Digitale Souveränität“ (2024): Hochschulen zwischen digitaler Souveränität und digitaler Abhängigkeit: Verunsicherung vs. Selbstbestimmung. Arbeitspapier Nr. 79. Berlin: Hochschulforum Digitalisierung. [https://hochschulforumdigitalisierung.de/wp-content/uploads/2024/06/HFD AP 79 AP-2024 digitale-Souveraenitaet_final-1.pdf](https://hochschulforumdigitalisierung.de/wp-content/uploads/2024/06/HFD_AP_79_AP-2024_digitale-Souveraenitaet_final-1.pdf)
- Bacharach, Guido, Jäger, Jakob, Wehnes, Harald (2023): Digitale Nachhaltigkeit: Digitale Souveränität und Open Source Software beim Einsatz von PM-Tools. Projektmanagement und Vorgehensmodelle 2023 - Nachhaltige IT-Projekte, Gesellschaft für Informatik e.V. <https://dl.gi.de/server/api/core/bitstreams/8514dec7-6058-4533-8f97-332940342819/content>
- Bundesministerium für Wirtschaft und Energie (BMWi) (2021): Schwerpunktstudie Digitale Souveränität, Berlin. https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/schwerpunktstudie-digitale-souveranitaet.pdf?__blob=publicationFile&v=1
- Bundesministerium für Wirtschaft und Klimaschutz (BWMK) (2018): Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen. https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p2-digitale-souveraenitaet-und-kuenstliche-intelligenz.pdf?__blob=publicationFile&v=1
- IT-Planungsrat (2021): Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung, Frankfurt am Main. https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf
- Kompetenzstelle Öffentliche IT (ÖFIT) (2017): Digitale Souveränität, Berlin. <https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t>
- Leiter der Rechen- bzw. Informationszentren der Universitäten des Landes Baden-Württemberg (2012): Umsetzungskonzept der Universitäten des Landes Baden-Württemberg für das Hochleistungsrechnen. <http://dx.doi.org/10.15496/publikation-21185>
- Leiterinnen und Leitern der Rechenzentren bzw. Informationszentren der Universitäten des Landes Baden-Württemberg (2019): Umsetzungskonzept der Universitäten des Landes Baden-Württemberg für das High Performance Computing (HPC), Data Intensive Computing (DIC) und Large Scale Scientific Data Management (LS² DM) <http://dx.doi.org/10.15496/publikation-27872>
- Rechnungshof Baden-Württemberg (2022): Denkschrift 2022, Karlsruhe. https://rechnungshof.baden-wuerttemberg.de/fileadmin/Denkschriften/Denkschrift_2022.pdf
- Sachverständigenrat für Verbraucherfragen (2017): Digitale Souveränität, Berlin. <https://core.ac.uk/download/pdf/132283323.pdf>
- Wissenschaftsrat (2023): Empfehlungen zur Souveränität und Sicherheit der Wissenschaft im digitalen Raum, Köln. <https://doi.org/10.57674/m6pk-dt95>