Einschätzung der Digitalen Souveränität an der UR

Stand: 20.04.2026

1. Digitale Souveränität an der UR

1.1. Begriffsverständnis

Mit der fortschreitenden Digitalisierung und der zunehmenden Integration von Informationstechnologie in operative Prozesse gewinnt der Begriff der Digitalen Souveränität zunehmend an Bedeutung. Organisationen sind heute in hohem Maße auf IT-Systeme, Daten und IT-Infrastrukturen angewiesen, um ihre Aufgaben erfüllen zu können. Gleichzeitig führen technologische Abhängigkeiten, komplexe IT-Ökosysteme und dynamische Marktstrukturen zu neuen Herausforderungen für eine langfristig stabile und verlässliche Gestaltung digitaler Infrastrukturen.

Vor diesem Hintergrund wird die aktive und nachhaltige Gestaltung der digitalen Umgebung zu einer zentralen Aufgabe von Organisationen, um ihre Handlungsfähigkeit im digitalen Raum dauerhaft zu sichern. Dabei steht Digitale Souveränität im Kern für die Unabhängigkeit, Eigenverantwortung und Selbstbestimmtheit von Akteuren in der digitalen Welt.

1.2. Struktur und Bemessungsgrundlagen

Digitale Souveränität bildet auch für die UR eine essenzielle strategische Voraussetzung zur nachhaltigen Sicherung ihrer Handlungsfähigkeit. Sie bezeichnet die Fähigkeit, IT-Systeme, Prozesse und IT-Infrastrukturen im Einklang mit strategischen Zielen selbstbestimmt steuern und weiterentwickeln zu können. Dabei betrifft die **technologische Selbstbestimmung** die technischen Komponenten (u. a. IT-Systeme, Daten, Infrastrukturen, Schnittstellen), während sich die **organisationale Selbstbestimmung** auf institutionelle Strukturen, Entscheidungsprozesse, Zuständigkeiten sowie rechtliche Rahmenbedingungen bezieht. Ergänzend werden **flankierende Merkmale** berücksichtigt, die im Kontext der organisationalen und der technologischen Selbstbestimmung zusätzliche Relevanz besitzen.

Ausgehend vom Verständnis dieser drei Dimensionen und ihren jeweiligen Kernaspekten wurden Kriterien (vgl. **Tabelle 1**) zur Bemessung der Digitalen Souveränität der UR abgeleitet.

Kriterien	Konkretisierungen
Organisationale Selbstbestimmung	
Verfügung, Transparenz und Kontrolle über Daten	Ist jederzeit nachvollziehbar, wo, wie und durch wen Daten verarbeitet, gespeichert und genutzt werden?
	Gilt diese Gewährleistung über den gesamten Lebenszyklus der Daten?
	Werden Daten außerhalb der UR ohne Zustimmung für fremde Zwecke verwendet?
Nutzbarkeit alternativer Lösungen	Existieren gleichwertige, digital souveräne Lösungen?
	Besteht eine wirtschaftliche oder vertragliche Bindung an einen Anbieter?
	Wie vergleichbar ist die Alternative im Hinblick auf den Funktionsumfang?
	Führt die Nutzung der Alternative zu Anpassungsaufwand oder Beeinträchtigungen bestehender Arbeits- und Prozessabläufe?
	Sind die Systeme benutzerfreundlich und praxistauglich für unterschiedliche Nutzergruppen?
Technologische Selbstbestimmung	
Flexibilität der eigenen Infrastruktur	Lässt die Infrastruktur einen Wechsel zu einer alternativen Lösung zu?
	Wie aufwändig ist die Realisierung eines Wechsels?
Kompetenzen zum Betrieb	Ist für den Betrieb des Systems spezialisiertes Wissen erforderlich?
	Welche zusätzlichen Kompetenzen müssen aufgebaut werden?
	Besteht eine ausreichende Möglichkeit, externe Expertise (z. B. Beratung oder Betrieb) einzubinden?
Offenheit von Systemen und Infrastrukturen	Bietet das System offene Standards oder offene Schnittstellen?
	Bestehen Abhängigkeiten von bestimmten technologischen Standards?

Technische Datenhoheit und Sicherheit	Wo wird die Infrastruktur betrieben? Erfolgt die Verarbeitung auf souveränen und vertrauenswürdigen Infrastrukturen?
	Ist gewährleistet, dass keine Herausgabe oder Übermittlung von Daten – insbesondere an Stellen außerhalb der EU bzw. des EWR – erfolgt?
	Kann die IT- und Betriebssicherheit des Systems gewährleistet und aufrechterhalten werden?
	Besteht grundsätzlich die Möglichkeit eines Wechsels zu einer souveränen Infrastruktur?
	Können Daten durch verschlüsselte Übertragung und Speicherung gesichert werden?
Flankierende Merkmale	
Wirtschaftlichkeit	Welche Kosten fallen für eine alternative (souveräne) Lösung an? Personalkosten? / Betriebs- und Wartungskosten? / Lizenzkosten? / Potenzielle Kosten bzw. Schäden durch Systemausfälle?
Resilienz[1]	Sind zur Sicherstellung der Betriebskontinuität geeignete Maßnahmen etabliert?
	Existiert ein unabhängiges Backup (an der UR oder bei einem vertrauenswürdigen Cloudanbieter), das auf offenen Datenstandards beruht?
	Liegen Exitstrategien oder Wechselpläne zu alternativen Lösungen vor?
	Bestehen Notfall- und Wiederanlaufpläne, die regelmäßig getestet und aktualisiert werden?
	Sind klare Verantwortlichkeiten sowie kontinuierliche Bewertungs- und Entscheidungsprozesse zum Umgang mit Risiken festgelegt?

Tabelle 1: Kriterien zur Einschätzung der Digitalen Souveränität.

2. Statusanalyse der Digitalen Souveränität an der UR

Zur Durchführung der Statusanalyse wurden zunächst die kritischen IT-Systeme in den IT-Domänen der UR (Forschung und Transfer, Lehre und Weiterbildung, Campus Management, End User Management, IT-Servicemanagement und Infrastruktur) identifiziert. Dieser Schritt wurde durch die für die jeweiligen Domänen verantwortlichen IT-Architektinnen und IT-Architekten durchgeführt. Im nächsten Schritt wurden die für die Statusanalyse erforderlichen Informationen erhoben. Auf Basis dieser Ergebnisse wurden die Kriterien aus Tabelle 1 angewendet, um die digitale Souveränität der IT-Systeme in den sechs Domänen einzuschätzen. Die Ergebnisse der Statusanalysen werden nachfolgend in den **Kapiteln 2.1. bis 2.6.** dargestellt.

2.1. Forschung und Transfer

Im Rahmen der Domäne „Forschung und Transfer“ wurden der Publikationsserver, der Bibliothekskatalog, das elektronische Laborbuch sowie die elektronische Zeitschriftenbibliothek als kritische IT-Systeme identifiziert. Für alle vier Systeme ist die Verarbeitung und Nutzung von Systemdaten über den gesamten Lebenszyklus hinweg transparent und nachvollziehbar. Bestimmte Daten können aufgrund der Forderungen von Open Science nachgenutzt werden. Ein Wechsel zu alternativen Lösungen würde weder zu einem Verlust wesentlicher Funktionalitäten noch zu einer Einschränkung der Benutzerfreundlichkeit führen, wäre jedoch mit geringfügigen Anpassungen an bestehenden Arbeits- und Prozessabläufen verbunden. Wirtschaftliche bzw. vertragliche Bindungen oder Erfordernisse an technische Infrastrukturen stehen einem möglichen Wechsel nicht entgegen.

Aufgrund von offenen Schnittstellen und standardisierten Metadaten können Daten bei der Migration ausgetauscht werden. Es besteht keine technologische Abhängigkeit. Die Infrastrukturen werden an der UR bzw. am Leibniz-Rechenzentrum (LRZ) betrieben. Daten, welche nicht öffentlich sind, werden nicht an Dritte übermittelt. Die IT-Sicherheit wird durch personelle und technische Unterstützung gewährleistet. Zusätzlich werden zwei Systeme (Elektronische Zeitschriftenbibliothek (EZB) und Publikationsserver) redundant an der UR und LRZ betrieben. Bei dem Bibliothekskatalog würden bei einer Alternativlösung Lizenzkosten anfallen, hier wurde erst auf die digital souveräne Lösung umgestellt. Durch eine Spiegelung am LRZ ist der Betrieb von zwei Systemen dauerhaft gewährleistet, beim Bibliothekskatalog wird diese vom LRZ und der Verbundzentrale des Bibliotheksverbund Bayern (BVB) gewährleistet. Für den Publikationsserver liegt eine Exitstrategie vor. Für alle Systeme gibt es Notfallpläne. Backups etc. werden regelmäßig überprüft, Daten auf den Servern des LRZ im Langzeitarchivierungssystem der Verbundzentrale des BVB am LRZ gespeichert.

[1] Resilienz bezeichnet die Fähigkeit, Störungen und Krisen zu bewältigen, die Funktionsfähigkeit unter veränderten Bedingungen aufrechtzuerhalten bzw. zeitnah wiederherzustellen und sich an neue und veränderte Rahmenbedingungen anzupassen.

Auf Grundlage dieser Feststellungen wird die Digitale Souveränität der Domäne „Forschung und Transfer“ als gewährleistet bewertet.

Fazit Kriterien	Organisatorische Selbstbestimmung	Technologische Selbstbestimmung	Wirtschaftlichkeit	Resilienz
Maßnahmen	-	-	-	-

Tabelle 1: Fazit für die Domäne "Forschung und Transfer".

2.2. Lehre und Weiterbildung

Im Rahmen der Domäne „Lehre und Weiterbildung“ wurden GRIPS, ILIAS und die Mediathek als kritische IT-Systeme identifiziert. Für alle drei Systeme ist die Verarbeitung und Nutzung von Systemdaten über den gesamten Lebenszyklus hinweg transparent und nachvollziehbar. Eine Datennutzung außerhalb der vorgesehenen Zwecke oder ohne Zustimmung erfolgt nicht. Ein Wechsel zu alternativen Lösungen würde weder zu einem Verlust wesentlicher Funktionalitäten noch zu einer Einschränkung der Benutzerfreundlichkeit führen, wäre jedoch mit geringfügigen Anpassungen an bestehende Arbeits- und Prozessabläufen verbunden. Wirtschaftliche bzw. vertragliche Bindungen oder Erfordernisse an technische Infrastrukturen stehen einem möglichen Wechsel nicht entgegen.

Der Migrationsaufwand wird für GRIPS und die Mediathek als hoch, für ILIAS als mittel eingeschätzt. Für den Betrieb von GRIPS und ILIAS ist kein spezialisiertes technisches Wissen erforderlich. Die Mediathek erfordert jedoch spezialisiertes Wissen und wird derzeit im Rechenzentrum der UR lediglich durch eine einzige Person betreut. Für GRIPS und ILIAS sind geeignete Maßnahmen zur Sicherstellung der Betriebskontinuität etabliert, welche für die Mediathek noch nicht umfänglich etabliert worden sind. Unabhängige Backups auf Basis offener Datenstandards sind bei GRIPS und der Mediathek vorhanden. Notfall- und Wiederanlaufpläne liegen für alle diese Systeme vor und werden regelmäßig getestet und aktualisiert.

Auf Grundlage dieser Feststellungen wird die Digitale Souveränität der Domäne „Lehre und Weiterbildung“ als gewährleistet bewertet. Eine wesentliche Einschränkung ergibt sich bezüglich der personellen Abhängigkeit bei der Mediathek, deren Betreuung in Zukunft durch weitere Mitarbeitende erfolgen sollte.

Fazit Kriterien	Organisatorische Selbstbestimmung	Technologische Selbstbestimmung	Wirtschaftlichkeit	Resilienz
Maßnahmen	-	*Betreuung der Mediathek durch weitere Mitarbeitende.*	-	*Maßnahmen der Betriebskontinuität für die Mediathek etablieren.*

Tabelle 2: Fazit für die Domäne "Lehre und Weiterbildung".

2.3. Campus Management

Durch die zuständigen IT-Architektinnen bzw. IT-Architekten wurden für die Domäne „Campus Management“ HISinOne, FlexNow, HIS-ERP, Lucom sowie D.3 DMS als kritische IT-Systeme betrachtet. Die Verarbeitung und Nutzung sämtlicher Systemdaten sind über den gesamten Lebenszyklus hinweg nachvollziehbar und transparent. Eine zweckfremde Nutzung ohne Zustimmung findet nicht statt. Vergleichbare Lösungen existieren für alle dieser Systeme und der Funktionsumfang ist jeweils vergleichbar. Allerdings bestehen vertragliche und wirtschaftliche Bindungen und ein Wechsel wäre mit größerem organisatorischen und migrationsbedingten Aufwand verbunden.

Die IT-Systeme dieser Domäne werden ohne Nutzung von Cloud-Komponenten auf Infrastrukturen des Rechenzentrums der UR betrieben. Sämtliche Anbieter der betrachteten Systeme haben ihren Sitz in Deutschland. Der Betrieb der Systeme erfordert durchgängig spezialisiertes Wissen und es bestehen technologische Abhängigkeiten von einzelnen Herstellern, wenngleich weitestgehend offene Standards und Schnittstellen genutzt werden. Die Betriebskontinuität ist durch etablierte Maßnahmen sowie regelmäßig überprüfte Notfall- und Wiederanlaufpläne abgesichert. Exitstrategien sowie durchgängig definierte Verantwortlichkeits- und Bewertungsstrukturen im Risikomanagement existieren jedoch bislang noch nicht.

Insgesamt betrachtet kann die Digitale Souveränität der Domäne „Campus Management“ als gewährleistet bewertet werden. Zukünftige Maßnahmen ergeben sich aus den Einschränkungen aus bestehenden Anbieterbindungen sowie aus fehlenden Verantwortungs- und Bewertungsstrukturen im Risikomanagement.

Fazit Kriterien	Organisatorische Selbstbestimmung	Technologische Selbstbestimmung	Wirtschaftlichkeit	Resilienz
Maßnahmen	*Abbau bestehender vertraglicher bzw. wirtschaftlicher Bindungen.*	-	-	*Etablierung von Exitstrategien und von Verantwortlichkeits- und Bewertungsstrukturen.*

Tabelle 3: Fazit für die Domäne "Campus Management".

2.4. End User Management

Beim „End User Management“ wurden das Mailsystem „GroupWise“, die Softwarebereitstellung, Storage-Dienste, Zoom, und Confluence als kritische IT-Systeme betrachtet. Bei den IT-Systemen ist die Verarbeitung der Systemdaten über den gesamten Lebenszyklus hinweg nachvollziehbar und transparent und es findet keine zweckfremde Nutzung der Systemdaten statt. Gleichwertige bzw. funktional überlegene Alternativen sind am Markt verfügbar. Es bestehen jedoch bei einzelnen Diensten vertragliche Bindungen und ein Wechsel der Anbieter würde großen organisatorischen Anpassungsaufwand und erheblichen Migrationsaufwand bedeuten. Die Benutzerfreundlichkeit einer alternativen Lösung wird nicht für alle Nutzergruppen als gegeben eingeschätzt.

Insbesondere bei GroupWise stellen Systemausfälle ein großes Problem und damit Einschränkungen bei Tätigkeiten in Forschung, Lehre und Verwaltung dar. GroupWise wird als On-Premise-Lösung am Rechenzentrum der UR betrieben, was spezialisiertes technisches Wissen und personelle Ressourcen erfordert. Dabei ist der Betrieb mit technologischen Abhängigkeiten verbunden. Offene Standards und Schnittstellen sind nur eingeschränkt umgesetzt. Die Datenübertragung erfolgt transportverschlüsselt via TLS. Eine verschlüsselte Speicherung der Daten erfolgt nicht, weil die Daten des Mailsystems auf Infrastrukturen am Rechenzentrum der UR liegen. Es sind Notfall- und Wiederanlaufpläne vorhanden. Exitstrategien und formal verankerte Bewertungs- und Entscheidungsprozesse sind jedoch nicht durchgängig etabliert. Die Backup-Struktur ist teilweise systemgebunden und damit nur eingeschränkt unabhängig.

Zusammenfassend weist die Domäne „End User Management“ insbesondere mit dem Mailsystem GroupWise Defizite auf, welche sich insbesondere aus der eingeschränkten Stabilität des Mailsystembetriebs ergeben. Auch im Hinblick auf Resilienz bestehen strukturelle Verwundbarkeiten, die zukünftig adressiert werden sollten.

Fazit Kriterien	Organisatorische Selbstbestimmung	Technologische Selbstbestimmung	Wirtschaftlichkeit	Resilienz
Maßnahmen	▪ *Abbau bestehender vertraglicher bzw. wirtschaftlicher Bindungen.* ▪ *Gewährleistung der kontinuierlichen Verfügbarkeit des Mailsystems.*	*Betrachtung weiterer Dimensionen außerhalb der Datenhoheit.*	-	▪ *Etablierung von Exitstrategien und Verantwortlichkeits- und Bewertungsstrukturen.* ▪ *Etablierung eines unabhängigen Backups für GroupWise.*

Tabelle 4: Fazit für die Domäne "End User Management".

2.5. IT-Servicemanagement

Die zuständigen IT-Architektinnen und IT-Architekten haben für die Domäne „IT-Servicemanagement“ das Ticketsystem Znuny als einziges kritisches IT-System bewertet. Die Verarbeitung der Systemdaten erfolgt über den gesamten Lebenszyklus hinweg transparent und nachvollziehbar. Eine zweckfremde Nutzung findet nicht statt. Es besteht eine vertragliche Bindung an den Anbieter. Vergleichbare Lösungen warten mit ähnlicher Benutzerfreundlichkeit und ähnlichem Funktionsumfang auf. Ein Wechsel würde nach Einschätzung mittleren Migrationsaufwand bedeuten, wenngleich im Falle einer Migration insbesondere zusätzliche Webentwicklungskompetenzen vorzuhalten wären.

Das Ticketsystem wird an der UR betrieben. Der Betrieb erfordert dabei spezialisiertes technisches Wissen. Offene Standards bzw. Schnittstellen sind grundsätzlich vorhanden. Die IT- und Betriebssicherheit ist im Rahmen der Sicherheitsstandards der UR gewährleistet. Es bestehen geeignete Maßnahmen zur Sicherstellung der Betriebskontinuität und es ist ein unabhängiges Backup auf Basis offener Datenstandards vorhanden. Verantwortlichkeiten und Bewertungsprozesse zum Umgang mit Risiken sind definiert und werden gelebt. Exitstrategien sowie Notfall- und Wiederanlaufpläne sind jedoch nicht etabliert. Auf dieser Basis ist die Digitale Souveränität der Domäne insgesamt gewährleistet.

Wenngleich im Bereich der Exitstrategien sowie der Notfall- und Wiederanlaufplanung noch Handlungsbedarf besteht, stehen im Falle eines Ausfalls des Ticketsystems alternative Supportkanäle zur Verfügung, über die IT-Serviceanfragen gestellt werden können. Der Handlungsbedarf ist in dieser Domäne daher insgesamt betrachtet als gering einzustufen.

Fazit Kriterien	Organisatorische Selbstbestimmung	Technologische Selbstbestimmung	Wirtschaftlichkeit	Resilienz
Maßnahmen	*Abbau bestehender vertraglicher bzw. wirtschaftlicher Bindungen.*	*Aufbau von zusätzlichen Webentwicklerkompetenzen*	-	*Etablierung von Exitstrategien und von Notfall- und Wiederanlaufplänen.*

Tabelle 5: Fazit für die Domäne "IT-Servicemanagement".

2.6. Intrastruktur

Auf Ebene der Infrastrukturen wurden Broadcom/VMWare, Omnissa, Opentext (File), SLES und Backup (IBM) bewertet. Für all diese Infrastrukturen ist die Datenverarbeitung über den gesamten Lebenszyklus hinweg nachvollziehbar. Eine zweckfremde Nutzung bzw. eine Nutzung von Systemdaten ohne Zustimmung findet über diese Infrastrukturen nicht statt. Zudem bestehen vertragliche und wirtschaftliche Bindungen, die einem Wechsel ebenso entgegenstehen würden wie ein als hoch bis sehr hoch eingeschätzter Migrationsaufwand.

Technologisch betrachtet werden alle diese Infrastrukturen an der UR betrieben. Sicherheitsanforderungen sowie verschlüsselte Datenübertragung und Datenspeicherung sind auf diese Weise umgesetzt. Der Betrieb der Infrastrukturen erfordert systemspezifisches technisches Fachwissen und ist mit technologischen Abhängigkeiten verbunden. Offene Standards oder Schnittstellen sind nicht durchgehend gegeben. Maßnahmen zur Sicherstellung der Betriebskontinuität sind etabliert, während sich Exitstrategien und Notfallpläne teilweise noch in Umsetzung befinden. Wirtschaftlich sind insbesondere hohe Migrationskosten sowie potenziell erhebliche Schäden im Falle eines Ausfalls zu berücksichtigen. Ein Wechsel zu alternativen Lösungen kann nach aktueller Einschätzung die bestehenden Defizite hinsichtlich digitaler Souveränität nicht beheben, da auch diese entsprechende Einschränkungen aufweisen.

Fazit Kriterien	Organisatorische Selbstbestimmung	Technologische Selbstbestimmung	Wirtschaftlichkeit	Resilienz
Maßnahmen	*Abbau bestehender vertraglicher bzw. wirtschaftlicher Bindungen.*	*Aufbau von zusätzlichen Webentwicklerkompetenzen*	-	*Etablierung von Exitstrategien und Notfallplänen.*

Tabelle 6: Fazit für die Domäne "Infrastruktur".