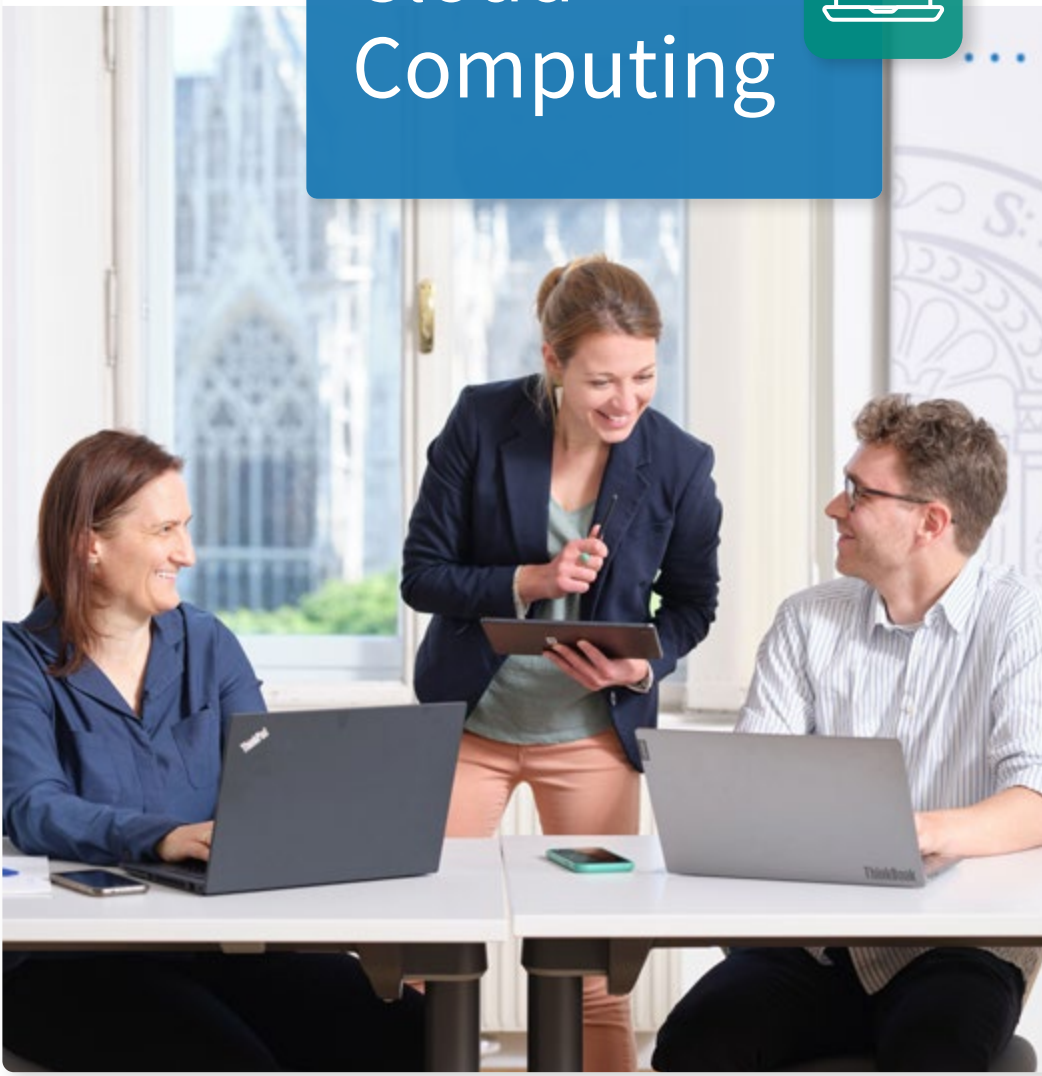
universität wien

Zentraler Informatikdienst

Cloud-Strategie der Universität Wien

Inhalt

Cloud-Computing



Eine allgemeingültige Annäherung an den Begriff Cloud-Computing bietet die Definition des National Institute of Standards and Technology (NIST, Bundesbehörde der Vereinigten Staaten für Standardisierung):

Cloud-Computing ist ein Modell, das den Zugriff auf einen geteilten Pool an konfigurierbaren IT-Ressourcen (etwa Netzwerke, Server, Speicherplatz, Anwendungen und Services) ermöglicht. Der Zugriff erfolgt bei Bedarf, ist jederzeit und von überall über ein Netzwerk möglich und zweckmäßig gestaltet. Die Ressourcen können rasch und mit minimalem Verwaltungsaufwand sowie mit minimaler Interaktion mit dem Anbieter bereitgestellt werden.

Dieses Cloud-Modell des NIST basiert auf essentiellen Charakteristika, Service- und Bereitstellungsmodellen, die im Folgenden beschrieben werden. Zu den **essenziellen Charakteristika** von Cloud-Computing zählen:

- **Selfservice:**
  Nutzer*innen können selbstständig IT-Ressourcen nach Bedarf nutzen. Dies geschieht automatisiert ohne menschliche Interaktion mit dem Anbieter des Dienstes.
- **Unabhängiger Zugriff:**
  Die Ressourcen sind über das Netzwerk verfügbar und durch Standard-Mechanismen abrufbar. Diese unterstützen die Nutzung über unterschiedliche Plattformen (Smartphones, Tablets, Laptops, PC, Smartwatches etc.).
- **Ressourcenpooling:**
  Die IT-Ressourcen des Anbieters (etwa Speicher, Rechenleistung oder Arbeitsspeicher) sind in einem Pool zusammengefasst, um mehrere Nutzer*innen bzw. Kunden bedienen zu können.
- **Elastizität:**
  Die IT-Ressourcen werden dynamisch bereitgestellt, um sich der Nachfrage schnell anzupassen. Nutzer*innen erscheinen die Ressourcen als unbeschränkt und jederzeit in unbegrenzter Menge verfügbar.
- **Messung und Kostenverrechnung:**
  Die Ressourcennutzung kann mittels an das Service angepasster Messverfahren (Speichermenge, Rechenleistung, Zahl aktiver Konten von Nutzer*innen etc.) gemessen und überwacht werden, etwa für die Abrechnung oder die automatische Skalierung der Ressourcen.

Bereitstellungsmodelle im Cloud-Computing sind:

- **Private-Cloud:**
  Eine Organisation bzw. deren Nutzer*innen (etwa Geschäftseinheiten) nutzen die Cloud-Infrastruktur exklusiv. Diese Organisation, ein Drittanbieter oder beide gemeinsam besitzen und betreiben die Private-Cloud.

- **Community-Cloud:**
  Die Cloud-Infrastruktur steht einer bestimmten Gemeinschaft von Nutzer*innen exklusiv zur Verfügung. Dieser Gemeinschaft gehören Organisationen mit ähnlichen Herausforderungen an, etwa in Bezug auf Sicherheitsanforderungen und Einhaltung nationaler Regelungen. Eine oder mehrere Organisationen dieser Gemeinschaft, ein Drittanbieter oder eine Kombination dieser Akteure besitzen und betreiben die Community-Cloud.

- **Public-Cloud:**
  Die Cloud-Infrastruktur ist für die Öffentlichkeit zugänglich. Ein Unternehmen, eine akademische Institution, eine Regierungsorganisation oder eine Kombination dieser Akteure besitzen und betreiben die Public-Cloud.

- **Hybrid-Cloud:**
  Die Hybrid-Cloud setzt sich aus zwei oder mehreren unterschiedlichen Bereitstellungs-modellen von Cloud-Infrastruktur (Private-, Community- oder Public-Cloud) zusammen. Diese bilden zwar separate Einheiten, sind aber miteinander über standardisierte oder proprietäre Technologien verbunden, wodurch Portabilität von Daten und Anwendungen möglich ist.

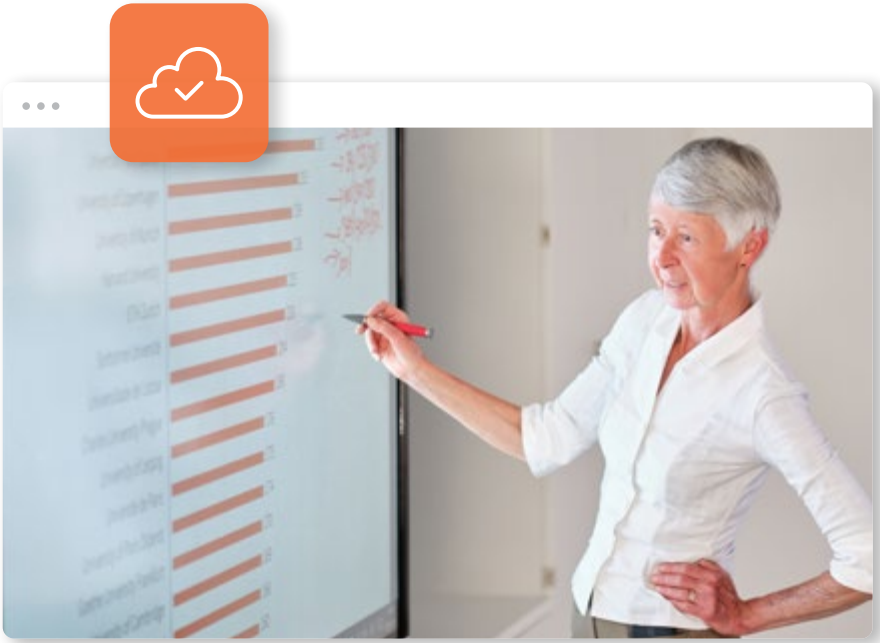
Folgende **Servicemodelle** stehen im Cloud-Computing zur Verfügung:

- **Software-as-a-Service (SaaS)**
  Dieses Servicemodell stellt Nutzer*innen die Anwendungen eines Dienstleisters zur Verfügung, die dieser auf einer Cloud-Infrastruktur betreibt. Diese Anwendungen sind von diversen Geräten zugänglich, etwa mittels Browser oder Programm-Interface.

- **Platform-as-a-Service (PaaS)**
  Im PaaS-Modell können Nutzer*innen eigens erstellte oder erworbene Anwendungen in einer Cloud-Infrastruktur einsetzen, solange diese Anwendungen mit jenen Programmiersprachen, Bibliotheken, Services und Werkzeugen erstellt wurden, die der Cloud-Anbieter unterstützt.

- **Infrastructure-as-a-Service (IaaS)**
  Das IaaS-Modell stellt Nutzer*innen Rechen-, Speicher-, Netzwerk- und andere grundlegende IT-Ressourcen bereit, auf denen sie jede Software und Betriebssysteme betreiben können.

(Quelle: Mell, P., & Grance, T. The NIST Definition of Cloud Computing.)



Mission-Vision-Statement

Durch die fortschreitende Digitalisierung wächst die Bedeutung von Cloud-Services. Die Universität Wien setzt sich zum Ziel im Spannungsfeld **Eigenentwicklungen und Eigenbetrieb** sowie Betrieb von Services in der **Cloud** die **nachhaltige** und **sichere Nutzung innovativer Cloud-Services für Forschung, Lehre und Verwaltung** an der Universität Wien zu ermöglichen.

Daten in der Cloud müssen **DSGVO-konform** und nach aktuellen Standards der **Informationssicherheit** verarbeitet werden. Dabei ist ein zweckmäßiger, sparsamer und **effizienter Ressourceneinsatz** zu wahren.

Um diese Strategie umsetzen zu können, müssen **Maßnahmen** in den Bereichen Ausbildung, Kompetenz sowie Technik gesetzt werden.

Strategie

Im Folgenden soll dargelegt werden, wie sich die Universität Wien zum Thema Cloud-Services in den strategischen Bereichen Innovation und Kompetenz, Wirtschaftlichkeit, Datenschutz und Informationssicherheit positioniert.

Innovation und Kompetenz

Innovation und Digitalisierung sind in vielen Bereichen eng miteinander verbunden. Deshalb ist es der Universität Wien ein wesentliches Anliegen, ihren Angehörigen aus Forschung, Lehre und Verwaltung **Zugang zu neuesten Technologien** zu ermöglichen.

Auf der einen Seite ist es für die Universität Wien essentiell, Eigen- und Weiterentwicklungen im digitalen Bereich zu fördern und **IT-Services selbst zu betreiben**. Dies ermöglicht, Wissen gebündelt an der Universität zu bewahren und zu mehren, technische Hintergründe zu verstehen und Entwicklungen selbst zu steuern und voranzutreiben.

Auf der anderen Seite finden heute **zahlreiche Entwicklungen** in der IT (etwa künstliche Intelligenz) **vorwiegend in der Public-Cloud** statt bzw. werden teilweise nur noch über Public-Cloud-Plattformen angeboten. Die Universität muss deshalb sicherstellen, dass Forscher*innen, Studierende und Mitarbeiter*innen auch auf diese innovativen Angebote Zugriff haben und sich an ihrer Anwendung und Weiterentwicklung beteiligen können.

Die **Ausbildung von Studierenden** macht es nötig, Innovationen im Bereich von Cloud-Computing mitzugestalten. Studierende müssen auf **neuen Cloud-Technologien** ausgebildet werden, da diese Plattformen in Unternehmen Standard sind. Großer Bedarf an neuen Technologien ist etwa an der Fakultät Informatik gegeben, da entsprechende Forschungs- und Lehrschwerpunkte zu Cloud-Services gesetzt wurden.

Wirtschaftlichkeit

Die Wirtschaftlichkeit der Nutzung von Private- und Public-Cloud-Ressourcen muss von der Universität Wien regelmäßig kritisch hinterfragt werden.

So wäre etwa eine Migration der gesamten IT-Infrastruktur in die Public-Cloud im Rund-um-die-Uhr-Betrieb bei einer Dimension wie jener der Universität Wien **nicht wirtschaftlich**.

Ein gutes **Beispiel** für deutlich höhere Kosten bei Auslagerung in die Cloud ist die **Storage-Infrastruktur** des ZID. Diese wird rund um die Uhr betrieben und ist auch in diesem Umfang verfügbar. Ein gleichwertiger Service via Cloud bereitgestellt würde die Kosten für die Universität Wien um ein Vielfaches erhöhen.

Auch sollte bedacht werden, dass die Einführung von neuen Cloud-Services nicht einfach nur eine Auslagerung von Services bedeutet, sondern damit vielmehr **zusätzliche Services** geschaffen werden, die **entsprechende Aufwände verursachen**:

- Neben den Gebühren für die Nutzung des Cloud-Services ist mit weiteren **Kosten** zu rechnen. So sind etwa **lokale Ressourcen** und gegebenenfalls **Personal** mit entsprechendem Know-how erforderlich, um diese Cloud-Services zu verwalten.
- Bei den vertraglichen Regelungen gilt es zu beachten, dass durch **Abhängigkeiten** von externen Anbietern keine **überhöhten Lizenzkosten** generiert werden.
- Ebenso muss die **Kompatibilität** dieserCloud-Services mit bestehenden Anwendungen an der Universität Wien sichergestellt werden.

Datenschutz

Werden interne Systeme in die Cloud migriert oder Services in der Cloud entwickelt, müssen

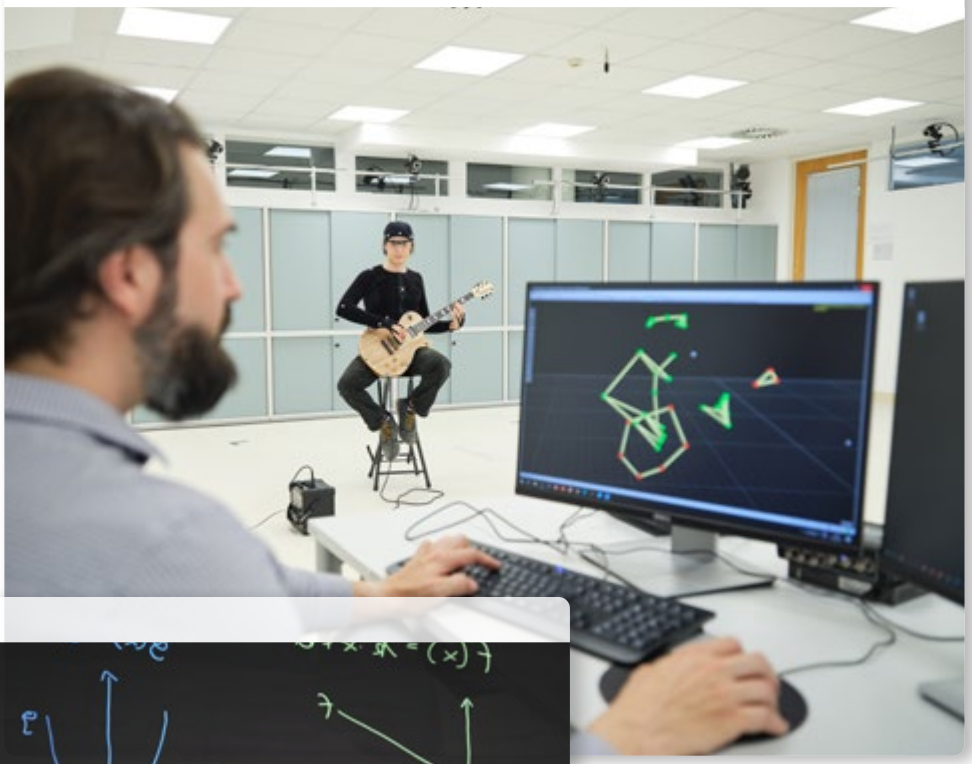
- die Vorschriften der **EU-Datenschutz-Grundverordnung** (EU-DSGVO) umgesetzt werden.
- die **Angehörigen** der Universität Wien ein **Bewusstsein** dafür entwickeln, dass die von ihnen genutzten und erstellten Daten wertige, sensible und kritische Ressourcen sind.
- die **Verarbeiter*innen** von Daten und die für die Datenverarbeitung **Verantwortlichen** für den ordnungsgemäßen Umgang mit Daten und dessen Dokumentation **sensibilisiert** werden.

Organisationseinheiten müssen ihre **Daten auswerten und bewerten**, wenn sie Cloud-Services einführen wollen. Dabei unterstützen sie folgende Werkzeuge:

- Der Prozess *Einführung eines Cloud-Services* gibt die nötigen Schritte dabei vor.
- Die Datenklassifizierung hilft zu bewerten, wie sensibel und kritisch die betreffenden Daten sind und wie groß das Risiko der Platzierung dieser Daten in der Cloud ist. Dies ist ein Indikator dafür, ob Daten auf eine Cloud-basierte Plattform migriert werden können.

Als Beispiel für die Herausforderungen, die sich bei Cloud-Services im Bereich Datenschutz und einem DSGVO-konformen Umgang mit Daten ergeben, kann wiederum die **Storage-Infrastruktur** des ZID herangezogen werden: Dort befinden sich sowohl **persönliche Daten**, die nach der EU-DSGVO als besonders schützenswert gelten, als auch **wissenschaftliche Daten** aus Lehre und Forschung, die aus Sicht der Universität Wien als schutzwürdig zu bewerten sind.

Auch wenn Public-Cloud-Anbieter verstärkt mit Datenzentren innerhalb der Europäischen Union und höchsten Standards in Bezug auf Sicherheit und Datenschutz werben, bleiben die datenschutzrechtlichen Herausforderungen bei der Nutzung von Cloud-Diensten bestehen. Zahlreiche **große Anbieter** am Cloud-Markt (Alibaba, Amazon, Microsoft, Google etc.) haben ihren **Firmensitz außerhalb der EU und fallen daher unter die Rechtsprechung des jeweiligen Landes**. Dies macht es relativ komplex, Public-Cloud-Services DSGVO-konform einzusetzen und nicht in Konflikt mit EU-Gesetzen zu geraten. Beispielsweise dürfen US-Behörden laut *Patriot Act* und *Cloud Act* Daten von Personen und Unternehmen von US-Cloud-Anbietern anfordern. Dies gilt auch dann, wenn sich die Server, auf denen die Daten gespeichert sind, außerhalb der USA befinden.



Informations-sicherheit

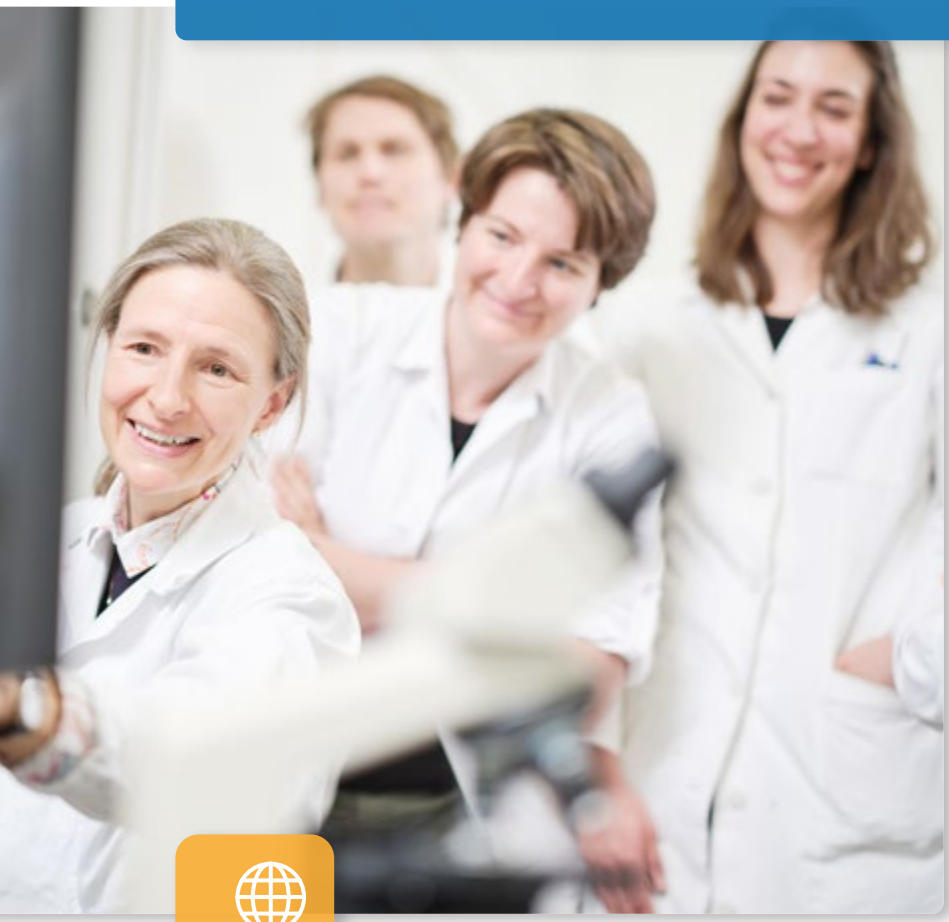
Bei der Auswahl und Nutzung von Cloud-Services müssen zahlreiche **Aspekte der IT-Security berücksichtigt** werden. Zusätzlich sind **operative Maßnahmen** für die Sicherheit der in der Cloud verarbeiteten Daten und Services durchzuführen.

Um die Informationssicherheit zu gewährleisten, werden zumindest folgende **Maßnahmen** bei der **Auswahl externer Cloud-Anbieter** empfohlen:

- Cloud-Anbieter und Cloud-Services evaluieren (insbesondere bezüglich Reputation, Ausfallsicherheit und Verfügbarkeit des Services)
- Verantwortliche für Sicherheitsmechanismen bestimmen (etwa für Backup der Daten)
- Security-Incident-Handling konzipieren
- Nutzer*innen-Management erarbeiten (Authentifizierung und Passworthoheit klären)
- Exit-Strategie entwerfen (Datenportabilität, wo benötigt, sicherstellen)

Da die Risiken beim **Betrieb virtueller Rechenzentren** in der Cloud (Infrastructure-as-a-Service) besonders hoch sind, sollte hier großes Augenmerk auf die Informationssicherheit gelegt und IT-Security-Verantwortliche mit entsprechenden Rechten ausgestattet werden. Etliche große Anbieter von IaaS (Amazon Web Services, Microsoft Azure etc.) haben hinsichtlich der Konfiguration und vor allem in Hinblick auf die Netzwerksicherheit eigene Best-Practices entwickelt, die es zu beachten gilt.

Verantwortlichkeiten



Die Einführung eines Cloud-Service an der Universität Wien bedingt die **Benennung eines*einer Serviceverantwortlichen** in der betreffenden Organisationseinheit. Der*die Serviceverantwortliche muss ein*e Mitarbeiter*in der Universität Wien sein und kann im Bedarfsfall eine*n Stellvertreter*in ernennen. Er*sie führt den **Prozess *Ein-führung eines Cloud-Service*** durch. Dieser Prozess umfasst die Bedarfsermittlung, eine Checkliste zur Analyse der Kernfragen der vier strategischen Bereiche sowie das Ausrollen des Service für die Nutzung (Kommunikation, Dokumentation).

Im Rahmen dieses Prozesses sind folgende Verantwortlichkeiten des*der Serviceverantwortlichen besonders hervorzuheben:

- **Datenschutz:**
  Die DSGVO-Konformität des einzuführenden Cloud-Service muss sichergestellt sein.
- **Finanzierung:**
  Für das einzuführende Cloud-Service muss eine finanzielle Freigabe vorliegen.
- **Informationssicherheit:**
  Die Maßnahmen zur Gewährleistung der Informationssicherheit, die bei der Auswahl des externen Cloud-Anbieters getroffen wurden, müssen dokumentiert werden.
- **Innerbetriebliche Regeln:**
  Die Einhaltung der relevanten Betriebsvereinbarungen muss gewährleistet sein.

Der*die Serviceverantwortliche ist in weiterer Folge für sämtliche Aspekte des Cloud-Service (etwa Dokumentation, Betrieb, Support) verantwortlich und dient als **Kontaktperson** bei Fragen zum Cloud-Service.

Impressum

Herausgeber
Universität Wien
Universitätsring 1
1010 Wien
www.univie.ac.at

Vizerektorat für Digitalisierung
und Wissenstransfer
DLE Zentraler Informatikdienst
Koordination Digitale Transformation
digital.zid@univie.ac.at

Foto-Credits
Joseph Krpelan (Cover)
Arnold Pöschl (S. 2, S. 3. S. 6, S. 8, S. 12, S. 14.)

Herbst 2021, Version 0.6