Cloud-Richtlinie

der Universität Passau

Beschlossen von der Universitätsleitung am 03.07.2024

RICHTLINIE FÜR CLOUD-DIENSTE

1. EINLEITUNG UND ZIELSETZUNG

Diese Richtlinie beinhaltet grundsätzliche Regelungen für alle Mitglieder der Universität Passau, die beabsichtigen, Cloud-Dienste zu nutzen. Sie informiert über allgemeine Risiken der Nutzung von Cloud-Diensten und hilft bei der Klärung der Frage, in welchen Fällen oder unter welchen Bedingungen Cloud-Dienste auf welche Art und Weise genutzt werden dürfen. Ausnahmen von den Vorgaben dieser Richtlinie sind durch die Universitätsleitung nach vorheriger Stellungnahme von Datenschutzbeauftragten und Informationssicherheitsbeauftragten festzulegen.

1.1 Begriffsdefinition

Cloud-Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die im Rahmen von Cloud-Computing angebotenen Dienstleistungen umfassen das komplette Spektrum der Informationstechnik und schließen unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software mit ein.

1.2 Vorteile, Erfolgsfaktoren und Risiken

Cloud-Computing bietet viele Vorteile: Die IT-Dienste können bedarfsgerecht, skalierbar und flexibel genutzt und je nach Funktionsumfang, Nutzungsdauer und Anzahl der Benutzer abgerechnet werden. Auch kann auf spezialisierte Kenntnisse und Ressourcen des Cloud-Dienstanbieters zugegriffen werden, wodurch interne Ressourcen für andere Aufgaben genutzt werden können. In der Praxis erfüllen sich jedoch häufig die Erwartungen, die mit der Cloud-Nutzung verbunden werden, nicht in vollem Umfang. Die Ursache hierfür ist meistens, dass wichtige kritische Erfolgsfaktoren im Vorfeld der Cloud-Nutzung nicht genügend berücksichtigt werden. Daher müssen Cloud-Dienste strategisch geplant sowie (Sicherheits-)Anforderungen, Verantwortlichkeiten und Schnittstellen sorgfältig definiert und vereinbart werden. Ein wichtiger Erfolgsfaktor sind zudem das Bewusstsein von und das Verständnis für die mit der Nutzung von Cloud-Diensten einhergehende(n) Änderung der Rollen sowohl auf Seite des IT-Betriebs als auch auf Seiten der Nutzerinnen und Nutzer der Institution, die den Cloud-Dienst einsetzt.

Insbesondere die dynamische Verteilung der Speicherkapazitäten über verschiedene Standorte, die den Nutzerrinnen und Nutzern in der Regel nicht bekannt sind, verlangen eine spezifische Vorsorge hinsichtlich der Informationssicherheit und des Schutzes der Daten.

Für die Verarbeitung personenbezogener Daten in der Cloud gelten insbesondere die Bestimmungen der EU-Datenschutz-Grundverordnung und des Bayerischen Datenschutzgesetzes. Die Cloud-Richtlinie stellt dar, wie diese gesetzlichen Vorgaben an der Universität Passau umgesetzt werden. Sie hilft den verantwortlichen Fachstellen, eigenständig Risiken zu erkennen, zu vermeiden und den die Cloud-Dienste gemäß den gesetzlichen Anforderungen und den an der Universität Passau geltenden Prozessen einzusetzen.

Im privaten Umfeld werden Cloud-Dienste vielfältig genutzt. Vor dem Hintergrund der sich zunehmend auflösenden Trennung von privaten und dienstlichen Belangen im IT- Bereich dient diese Richtlinie zudem als Handlungsanleitung zur Sensibilisierung gegenüber potentiellen Risiken.

2. GELTUNGSBEREICH

Diese Richtlinie gilt für alle Mitglieder und Angehörigen der Universität Passau, wenn sie im Rahmen dienstlicher Tätigkeiten (insbesondere für Verwaltung, Forschung und Lehre) Daten erheben, speichern oder in sonstiger Weise verarbeiten.

3. DIENSTEBEREITSTELLUNG

Für zentral bereitgestellte Dienste können spezifische Nutzungsbedingen festgelegt werden.

Die freigegebenen Dienste werden in geeigneter Form unter https://www.uni-passau.de/datenschutz/cloud den Mitgliedern der Universität Passau bekannt gegeben. Eine Freigabe kann auch nur befristet oder beschränkt auf Vertraulichkeitsklassen erfolgen. Die Nutzung bzw. die Fortsetzung einer Nutzung von Diensten kann an eine vorherige Einweisung, Sensibilisierung oder regelmäßige Fortbildungen geknüpft werden.

Eine Freigabe für Dienste oder Diensteklassen kann von den nach dem IT-Betreuungskonzept durch die von der Universität Passau bestimmten Verantwortlichen beschränkt oder aufgehoben werden. Soweit eine solche Maßnahme nicht der Abwendung unmittelbarer Gefahren dient, soll die Beschränkung oder Aufhebung der Freigabe mindestens einen Monat im Voraus angekündigt werden.

Dem Freigabeprozess liegt im Hinblick auf die vielfältigen Dienste-Anforderungsbedarfe an der Universität Passau folgende Basisklassifizierung zu Grunde. Dienste, die anonym ohne Preisgabe schützenswerter Informationen genutzt werden, sind vom Freigabeprozess ausgenommen.

Dienste-klasse	I	II	III	IV	V
Risiko-Wert	Besonders geringes Risiko	Geringes Risiko	Normales Risiko	Substanzielles Risiko	Hohes Risiko
Dienste-Art	Dienste, die Inhalte über eine Netzwerkverbindung nur nach Interaktion der Nutzerinnen und Nutzer zum Download bereitstellen	Dienste, die über eine Netzwerkverbindung Inhalte auch ohne Interaktion der Nutzerinnen und Nutzer bereitstellen	Dienste, die über eine Netzwerkverbindung die hochgeladenen Inhalte der Nutzerinnen und Nutzer nur temporär verarbeiten	Dienste, die über eine Netzwerkverbindung die hochgeladenen Inhalte der Nutzerinnen und Nutzer abspeichern aber nicht in sonstiger Form verarbeiten	Dienste, die über eine Netzwerkverbindung die hochgeladenen Inhalte der Nutzerinnen und Nutzer verarbeiten und nicht nur abspeichern
Komplexität, den Dienst zu beenden oder zu wechseln (Art. 10 BayDIG)	Es gibt zahlreiche bewährte Alternativen, die bereits parallel genutzt werden.	Es gibt einige bewährte Alternativen, die bereits parallel genutzt werden.	Es gibt einige bewährte Alternativen, die bereits parallel genutzt werden könnten.	Es bestehen nur wenigen Alternativen, die noch nicht in der Praxis bewährt sind.	Es bestehen keine bewährten Alternativen, ein Ausstiegsplan ist erforderlich
Umfang der Datenverarbeitung und der Anzahl	Datenverarbeitung auf wenige Daten beschränkt, leicht überschaubar.	Datenverarbeitung für den Verantwortlichen und Nutzer überschaubar.	Datenverarbeitung für den Verantwortlichen und Nutzer	Umfangreiche Datenverarbeitung nicht ausgeschlossen, Umfang	Umfangreiche Datenverarbeitung; Umfang der Verarbeitung

der Betroffenen	Nur einzelne Betroffene	Nur einzelne Betroffene, jedoch weniger Kontrolle durch die Universität	noch überschaubar. Drittbetroffene denkbar	für den Verantwortlichen und Nutzer teilweise überschaubar. Drittbetroffene denkbar	für den Verantwortlichen und Nutzer nicht überschaubar. Regelmäßig Drittbetroffene
Informations-sicherheit	Kein Unterschied zum verantwortungsbewussten Surfen im Internet	Gefährdung der Integrität denkbar	Wohl kein dauerhafter Abfluss von Informationen	Abfluss von Informationen nicht ausschließbar, aber Schutzmöglichkeiten vorhanden	Abfluss von Informationen und Prozessen
Beispiel	Microsoft eigene Onlinebilder in Office einfügen Adobe Stock Bilder	Automatische Updates	Übersetzer in Microsoft Office, Dropbox, jedoch mit vorab verschlüssel-ten Daten	Microsoft OneDrive, Zoom Cloudaufzeichnung und Whiteboard	Automatisierung von Workflows mit PowerAutomate in Microsoft 365

Für die Prozesse, die durch den Dienst unterstützt werden, ist eine Dokumentation der **Verarbeitungstätigkeit** zu erstellen.

Für Dienste ab der Klasse III sind frühzeitig im Rahmen der Beschaffung der / die Datenschutzbeauftragte und der / die Informationssicherheitsbeauftragte einzubeziehen; im Regelfall ist der Abschluss einer **Vereinbarung zur Auftragsverarbeitung** mit dem Diensteanbieter erforderlich.

Für Dienste unterhalb der Klasse III sind Datenschutzbeauftrage und Informationssicherheitsbeauftrage spätestens mit dem Einsatz über den Dienst zu informieren. Im Einzelfall kann auch der Abschluss einer Vereinbarung zur Auftragsverarbeitung mit dem Diensteanbieter erforderlich sein.

4. SICHERHEITSMAßNAHMEN

Angehörige und Mitglieder der Universität Passau sind aufgefordert, folgende Sicherheitsmaßnahmen bei der Nutzung von Cloud-Diensten zu berücksichtigen.

4.1 Sparsamer Umgang

Prinzipiell sollten bei der Nutzung von Cloud-Diensten die in Frage kommenden Datenmengen auf das notwendige Mindestmaß begrenzt werden. So kann beispielsweise bei der Übertragung ganzer Verzeichnisbäume in die Cloud leicht übersehen werden, dass in einem Unterverzeichnis sensible Daten abgelegt wurden, die den Bereich der Universität Passau nicht verlassen dürfen.

4.2 Vorrangig zentral verwaltete Dienste der Universität Passau nutzen

Services, die von der Universität Passau-IT zentral bereitgestellt werden, sind sonstigen Cloud-Diensten externer Anbieter vorzuziehen. Nur wenn der benötigte Dienst nicht von der Universität Passau bereitgestellt wird oder der bereitgestellte Dienst den Anforderungen nicht genügt, darf unter Beachtung der hier formulierten Grundsätze auf Angebote externer Anbieter zurückgegriffen werden.

4.3 Verschlüsselungsqualität

Die jeweilige erforderliche Verschlüsselung muss nach dem Stand der Technik erfolgen, soweit möglich orientiert an der jeweils aktuell gültigen technischen Richtline des Bundesamtes für Sicherheit in der Informationstechnik, insbesondere der Richtlinie 02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Für die Qualität der Verschlüsselung müssen ausreichenden vertragliche Garantien oder Nachweise der Cloud-Dienste-Anbieter vorliegen. ZIM und Datenschutzbeauftragte können bedarfsangemessen beratend unterstützen.

5. Schutzbedarf

Aus dem Schutzbedarf der für eine Auslagerung vorgesehenen Daten folgt nicht nur, ob eine Auslagerung zulässig ist, sondern auch unter welchen Bedingungen dies geschehen kann. Dabei ist der Schutzbedarf getrennt nach den drei Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit zu betrachten.

5.1 Maßnahmenart nach Diensteklassen

Neben den technischen und organisatorischen Maßnahmen des Anbieters müssen ab Dienstklasse III eigene organisatorische Maßnahmen zur Risikobehandlung durch die jeweilige(n) Dienststelle bzw. Dienststellen (Abteilung/Referat/wissenschaftliche Einrichtung) festgelegt werden, die diesen Dienst einsetzen. Bei Dienste Klasse IV und V müssen auch eigene technische Maßnahmen zur Risikobehandlung getroffen werden. Zu möglichen Maßnahmen beraten Informationssicherheitsbeauftragte und Datenschutzbeauftragte.

5.2 Verfügbarkeit

Es muss vorab geprüft werden, welche Aussagen der Anbieter des Cloud-Dienstes zur Gewährleistung der Verfügbarkeit macht. Wenn sehr hohe Anforderungen an die Verfügbarkeit bestehen, kommt eine Datenablage in der Cloud nur dann in Frage, wenn der Anbieter des Cloud-Dienstes eine entsprechend hohe Verfügbarkeit garantiert.

5.3 Integrität

Die Unverfälschbarkeit der Daten (Integrität) wird im Allgemeinen von Anbietern von Cloud-Speichern nicht garantiert. Wenn in dieser Hinsicht hohe oder sogar sehr hohe Anforderungen bestehen, muss der Nutzer selbst geeignete Maßnahmen zur Gewährleistung der Integrität ergreifen. Beispielsweise können Prüfsummen verwendet werden, mit deren Hilfe eine Veränderung an den Daten erkannt werden kann. In Systemen zur Datenverschlüsselung (siehe nachfolgender Absatz) sind derartige Verfahren in der Regel bereits integriert.

5.4 Vertraulichkeit

Wenn hohe Anforderungen an die Vertraulichkeit gestellt werden, ist als adäquate Maßnahme der Einsatz eines Datenverschlüsselungssystems zwingend notwendig. Viele Anbieter von Speicherplatz in der Cloud bieten auch Dienste zur Datenverschlüsselung an. Bei der Nutzung

dieser Verschlüsselungsdienste ist in der Regel nicht zuverlässig nachvollziehbar, wer Zugriff auf die Schlüssel und damit auf die Daten hat. Der Zugriff des Dienstanbieters auf die Schlüssel muss ausgeschlossen sein. Darum sollte die Verschlüsselung selbst durchgeführt werden, bevor die Daten in die Cloud übertragen werden. Die Sicherheit verschlüsselter Daten hängt u.a. von der Qualität des Verschlüsselungsalgorithmus, der Verschlüsselungssoftware, der Schlüssellänge und dem Schlüsselmanagement ab. Beim Einsatz von Verschlüsselung muss darauf geachtet werden, dass sie nach allgemein anerkannten Regeln und dem aktuellen Stand der Technik als sicher gilt.

Für die Entscheidung, welche Daten auf welche Art und Weise bei Cloud-Diensten gespeichert werden können, sind folgende Klassifizierungsstufen V1 bis V4 und Maßnahmen vorgesehen:

Vertrau-lichkeits-stufe	**öffentlich (V1)**	**intern (V2)**	**vertraulich (V3)**	**Streng vertraulich (V4)**
Informa-tions-gruppe	Beispiele: Vorlesungs-verzeichnis, Presse-mitteilungen, Flyer, öffentliche Teile der Webseite, öffentliche Veranstaltungs-programme, Publikationen	Beispiele: Intranet, Regelwerke, Arbeitsan-weisungen, interne Telefonverzeich-nisse, interne Veranstaltungen, unveröffentlichte Forschungsdaten	Beispiele: Dokumente mit vertraulichen personenbezogen en Daten, Reiskosten-abrechnungen, techn. Daten (Baupläne sensibler Räume, Netzwerkpläne), geschützte Studienarbeiten, Prüfungswesen	Beispiele: Studierenden-akten, Personalakten, Datenverarbeitung in Zusammenarbeit mit Dritten (Militär, Forschung, Wirtschaft), aus einer gesetzlichen, dienstlichen oder vertraglichen Verpflichtung als streng vertraulich zu behandelnden Daten

5.5 Rechtliche Rahmenbedingungen

5.5.1 Vorgaben und Rechtsvorschriften

In allen Fällen sind die folgenden Aspekte zu beachten:

- Soweit ein Dienst für die Verarbeitung von Forschungsdaten genutzt wird, sind Datenmanagementpläne bereitzuhalten. Diese sollen sich an den Leitfäden von SCIENCE EUROPE orientieren.
- Für personenbezogene Daten (sowohl mit dienstlichem als auch privatem Bezug) gelten die Bestimmungen des Datenschutzes, insbesondere der EU-Datenschutz-Grundverordnung.
- Wurden Informationen von Dritten im Rahmen dienstlicher Tätigkeit anvertraut, ist § 203 StGB zu beachten.
- Steuerrechtlich relevante Unterlagen sind auf dem Gebiet der Europäischen Union zu speichern.

- Geheimisse gelten nach dem Gesetz zum Schutz von Geschäftsgeheimnis rechtlich nur dann als geschützt, wenn angemessene Maßnahmen zu deren Schutz ergriffen worden sind.

In seltenen Fällen sind die Vorgaben für Verschlusssachen zu beachten, insbesondere das Bayerisches Sicherheitsüberprüfungsgesetz.

5.5.2 Informationen / Daten der Vertraulichkeitsstufen V1 und V2

Informationen der Klassen V1 und V2 können in internen und externen Clouds unverschlüsselt gespeichert werden.

Bei internen Informationen (V2) darf weiterhin der Zugriff nur für berechtigte Mitglieder und Angehörige der Universität Passau möglich sein.

5.5.3 Daten der Vertraulichkeitsstufe V3

Informationen der Klassen V3 dürfen nur in bereits verschlüsselter Form bei externen Cloud-Anbietern gespeichert werden. Im Rahmen einer Freigabe kann von dem Erfordernis der Verschlüsselung abgesehen werden.

5.5.4 Daten der Vertraulichkeitsstufe V4

Informationen der Klassen V4 dürfen nicht bei externen Cloud-Anbietern gespeichert werden.

5.6 Löschung von Daten

Anbieter von Cloud-Diensten setzen normalerweise Speichertechniken zur effizienten Ausnutzung der physikalischen Speicherkapazitäten ein. Dadurch können Daten oft erst nach einer gewissen Zeitspanne gelöscht werden. Grundsätzlich kann nicht ausgeschlossen werden, dass durch die Betätigung des Löschbefehls die Daten zwar für den Anwender nicht mehr sichtbar sind, diese aber nicht gelöscht wurden. Daher sind Daten, die beispielsweise einer gesetzlichen Löschverpflichtung unterliegen, nur dann für die Ablage in der Cloud geeignet, wenn entsprechende vertragliche Garantien hinsichtlich der effektiven Löschung vorliegen.