Universität Regensburg

Cloud-Richtlinie

Richtlinie der Universität Regensburg zur Auslagerung von Daten in Cloud-Diensten

Inhaltsverzeichnis

Steckbrief

Zielsetzung	Umgang mit Cloud-Diensten
Inhalt	Regelungen zur Speicherung von Daten in der Cloud
Zielgruppe	Alle Mitglieder der Universität Regensburg
Geltungsbereich	Alle Tätigkeiten der UR
Gültigkeitsdauer	Unbefristet

1. Einleitung

Diese Richtlinie beinhaltet grundsätzliche Regelungen für alle Mitglieder der Universität Regensburg (UR) die im Rahmen ihrer Tätigkeit öffentliche Cloud-Dienste (so genannte Public Clouds) zur Datenablage nutzen wollen. Sie soll der Sensibilisierung dienen, informiert über allgemeine Risiken und hilft bei der Klärung der Frage, in welchen Fällen oder unter welchen Bedingungen Cloud-Dienste genutzt werden dürfen.

Wenn Daten mit Hilfe von Cloud-Diensten gespeichert bzw. verarbeitet werden, drohen spezielle Gefahren. Insbesondere die dynamische Verteilung der Speicherkapazitäten über verschiedene Standorte, die in der Regel dem Nutzenden nicht bekannt sind, verlangen eine spezifische Vorsorge hinsichtlich der Informationssicherheit und des Schutzes der Daten.

Für die Verarbeitung personenbezogener Daten in der Cloud gelten die Bestimmungen der EU-Datenschutz-Grundverordnung (EU-DSGVO).

Im privaten Umfeld werden Cloud-Dienste häufig relativ sorglos genutzt. Vor dem Hintergrund der sich immer mehr auflösenden Trennung von privaten und studentischen/wissenschaftlichen Belangen, speziell im IT-Umfeld, soll diese Richtlinie zur Sensibilisierung gegenüber den potentiellen Risiken beitragen und entsprechende Handlungsanleitungen geben.

1.1 Geltungsbereich

Diese Richtlinie gilt für alle Mitglieder der Universität Regensburg, wenn sie im Rahmen ihre Tätigkeiten für die UR Daten erheben, speichern oder verarbeiten.

1.1 Abgrenzung und Begriffsdefinition

IT-Dienste, die unabhängig von Ort und Zeit über ein Daten- oder Kommunikationsnetz genutzt werden können, werden allgemein als „Cloud Computing“ bezeichnet. Allerdings existieren verschiedene leicht variierende Definitionen des Begriffs. Im Folgenden benutzen wir eine Begriffsdefinition, die sich an die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) festgelegte Definition des Begriffs Cloud Computing anlehnt:

„Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. In der Regel können diese IT-Dienstleistungen unabhängig von Ort und Zeit mit Hilfe aller gängigen IT-Geräte genutzt werden. Für die Nutzer bleibt die bereitgestellte IT-Infrastruktur verborgen.“ [2]

Diese Richtlinie betrachtet Aspekte der Speicherung von Daten, also der kurzzeitigen oder längerfristigen Überlassung von Daten an externe Dienstanbieter, mit Hilfe von Cloud Services. Weitere Cloud-Angebote, wie zum Beispiel Office-Dienste oder Rechenleistung, werden nicht behandelt.

2. Datenkategorien und ihre Eignung zur Cloud-Nutzung

Für die Entscheidung, unter welchen Bedingungen eine Auslagerung von Daten in die Cloud in Frage kommt, bildet der Schutzbedarf der Daten die grundlegende Richtschnur (siehe Anhang I. Schutzklassen mit Schutzbedarf). Daten lassen sich in die folgenden Klassen einteilen:

Schutz-klasse	Beispiele	Vertraulichkeits-stufe	Schutz-bedarf
0	Daten, die aus öffentlichen zugänglichen Quellen stammen	öffentlich	Keinen
1	Wissenschaftliche Daten, sofern sie für Dritte nicht interpretierbar sind	intern	Normal bis hoch
2	Wissenschaftliche Daten (z.B. Untersuchungsergebnisse, Messreihen)	vertraulich	Hoch bis sehr hoch
	Dienstliche (nicht wissenschaftliche) Daten (z.B. aus der Bereich der Verwaltung und Lehre)	vertraulich	Hoch bis sehr hoch
3	Personalaktendaten	geheim	Sehr hoch

In jedem Fall sind die folgenden Aspekte zu beachten:

- Für personenbezogene Daten (sowohl mit dienstlichem als auch privatem Bezug) gelten die Bestimmungen des Datenschutzes.
- Auch Daten ohne Personenbezug können einen sehr hohen Schutzbedarf haben (zum Beispiel auf Grund von Geheimhaltungsvereinbarungen).

Ein Schutzbedarf wird grundsätzlich hinsichtlich der drei Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit differenziert bestimmt. Entsprechend differenziert müssen Vorkehrungen zur Sicherheit der Daten getroffen werden. Aus dem Schutzbedarf der Daten folgt zwingend die Eignung oder Nicht-Eignung zur Speicherung in der Cloud:

Schutzbedarf	Eignung für die Ablage
Daten, mit keinem oder normalen Schutzbedarf	Ja, für die Ablage geeignet
Daten mit hohem Schutzbedarf	Nur für die verschlüsselte Ablage geeignet
Daten mit sehr hohem Schutzbedarf	Nein, nicht für die Ablage geeignet

Insbesondere dürfen die folgenden Daten nicht in der Cloud abgelegt werden:

Personalaktendaten	Nein, nicht für die Ablage geeignet
Dienstliche Daten mit Personenbezug	Nein, nicht für die Ablage geeignet
Haushaltsdaten	Nein, nicht für die Ablage geeignet

3. Regelungen

Bevor Daten in der Cloud abgelegt werden, müssen die im vorangegangenen Abschnitt 2 betrachteten Abhängigkeiten zwischen der Datenkategorie, dem Schutzbedarf der Daten und daraus resultierenden Eignung beachtet werden. Darüber hinaus gelten die in diesem Abschnitt aufgestellten Regelungen.

3.1 Sparsamer Umgang

Prinzipiell sollten bei der Nutzung entsprechender Cloud-Dienste, die in Frage kommen, die Datenmengen auf das notwendige Mindestmaß begrenzt werden. Beispielsweise kann bei der Übertragung ganzer Verzeichnisbäume in die Cloud leicht übersehen werden, dass in einem Unterverzeichnis sensible Daten abgelegt wurden, die den Netzwerkbereich der UR nicht verlassen dürfen. Bevor Daten auf Speichersysteme externer Anbieter ausgelagert werden, müssen erwarteter Nutzen und damit verbundene Risiken gegeneinander abgewogen werden.

3.2 Vorrangig Dienste der UR nutzen

Vorrangig sind für die Speicherung und Verarbeitung von wissenschaftlichen und dienstlichen Daten die von der Universität Regensburg bereitgestellten und freigegebenen Systeme (MyFiles bzw. BayernShare) zu nutzen.

- Eine Speicherung und Verarbeitung von nicht für die Öffentlichkeit bestimmten Informationen (ab hohem Schutzbedarf) in nicht von der Universität Regensburg bereitgestellten Cloud-Speicher Diensten (wie OneDrive) ist grundsätzlich nicht gestattet.
- UR-Zugangsdaten dürfen nicht bei Dritten verwendet oder hinterlegt werden.

Nur unter Beachtung der hier formulierten Grundsätze darf auf vom RZ freigegeben Cloud-Dienste (wie OneDrive) zurückgegriffen werden.

3.3 Schutzbedarf der Daten bestimmt den Umfang der Cloud-Nutzung

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:

3.3.1 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 vorgenommen werden, bevor die Daten in die Cloud übertragen werden. Die Sicherheit verschlüsselter Daten hängt u.a. von der Qualität des Verschlüsselungsalgorithmus, der Verschlüsselungssoftware, der Regelungen, Schlüssellänge und dem Schlüsselmanagement ab. Beim Einsatz von Verschlüsselung muss darauf geachtet werden, dass sie nach allgemein anerkannten Regeln als sicher gilt.

Bei Daten mit *sehr hohen Anforderungen* an die Vertraulichkeit ist grundsätzlich von der Ablage in der Cloud abzusehen.

3.3.2 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 Absatz 3.3.1 - Vertraulichkeit) sind derartige Verfahren in der Regel bereits integriert.

3.3.3 Verfügbarkeit

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

3.4 Löschung von Daten

Anbieter von Cloud-Speicher setzen normalerweise Speichertechniken zur effizienten Ausnutzung der physikalischen Speicherkapazitäten ein. Aufgrund dieser Speichertechnik können Daten oft erst nach einer gewissen Zeitspanne gelöscht werden. Grundsätzlich kann nicht ausgeschlossen werden, dass beim Absetzen des Löschbefehls die Daten lediglich für den Anwender ausgeblendet, aber nicht gelöscht werden. Daher sind Daten, die einer beispielsweise gesetzlichen Löschverpflichtung unterliegen, für die Ablage in der Cloud ungeeignet.

3.5 Dienstrechtliche Vorgaben beachten

Insbesondere für Daten der Verwaltung (vor allen Dingen Personal- und Haushaltsdaten) existieren oft detaillierte Vorschriften, die den Umgang mit den Daten regeln. Beispielsweise regeln verschiedene Vorschriften, dass Personalakten die Personalabteilung nicht ohne weiteres verlassen dürfen. Somit dürfen derartige Personaldaten auch nicht auf Speicher außerhalb der UR abgelegt werden. Inwieweit bei der Datenspeicherung dienstrechtlich Vorschriften zu beachten sind, muss im Zweifel unter Einbeziehung des jeweiligen Vorgesetzten geklärt werden.

3.6 UR-interne Regelungen beachten

Für bestimmte Systeme (MS 365, Trello etc.) können bei Bedarf ergänzende Benutzungsrichtlinien festgelegt werden.

Als Ergänzung oder Konkretisierung gesetzlicher Bestimmungen und Vorschriften gilt eine Reihe von weiteren universitätsinternen Regelwerken.

4. Schlussbestimmungen

4.1 Bekanntmachung

Diese Richtlinie ist allen Mitgliedern der Universität in geeigneter Weise zugänglich zu machen, insbesondere über das Intranet. Eine allgemeine Veröffentlichung dieser Richtlinie ist nicht vorgesehen, da es sich um eine interne Richtlinie handelt.

4.2 Gültigkeit und Dokumenten-Handhabung

Die Leitung des Rechenzentrums behält sich das Recht vor, diese Richtlinie bei Bedarf zu ändern. Änderungen können insbesondere erforderlich werden, um gesetzlichen Vorgaben, bindenden Verordnungen, Forderungen der zuständigen Aufsichtsbehörde oder internen Verfahren der Universität Regensburg zu entsprechen.

Der/die Verantwortliche für dieses Dokument ist der/die IT-Sicherheitsbeauftragte, welche/r die Richtlinie in regelmäßigen Abständen auf inhaltliche Richtigkeit und Konsistenz mit anderen Richtlinien, Handlungsanweisungen, etc. prüft und aktualisiert. Nach Freigabe muss die nächste Überprüfung spätestens nach 4 Jahren erfolgen.

4.3 Inkrafttreten

Diese Richtlinie tritt am Tage nach ihrer Bekanntmachung in Kraft und ist für alle Mitglieder der Universität Regensburg verbindlich.

Regensburg, den 27.04.2021
Universität Regensburg

Gez.
Dr. Christoph Bauer
Komm. Leiter Rechenzentrum

Anhang

I. Schutzklassen mit Schutzbedarf

Schutzklassen (+Beispiele)	Schutz-bedarf	Anforderungen an TOMs nach BSI „IT-Grundschutz“
Schutzklasse 0 (öffentlich)		**Keine Absicherung**
Vorgänge, die keine oder keine schutzbedürftigen Aussagen über persönliche Verhältnisse nat. Personen enthalten, erzeugen, unterstützen oder solche ermöglichen oder die von den Betroffenen frei zugänglich gemacht wurden. ➞ Keine besondere Beeinträchtigung und von den Betroffenen frei zugänglich gemacht worden. *Synthetisch erzeugte Testdaten (Max Mustermann), wirksam aggregierte Daten, vom Betroffenen freigegebene Daten, Arbeitsanweisungen auf UR-Webseite, Leitlinien, Formulare, dienstliches Telefonverzeichnis*	Kein	Keine Absicherung nach BSI erforderlich.
Schutzklasse 1 (intern)		**Basis-Absicherung**
Vorgänge, die durch einbezogene Daten und konkrete Verarbeitung dieser Aussagen über persönliche Verhältnisse des Betroffenen enthalten, erzeugen, unterstützen oder solche ermöglichen. ➞ Keine besondere Beeinträchtigung, von den Betroffenen nicht frei zugänglich gemacht worden. *Name, Anschrift (ohne Kontext), Staatsangehörigkeit (ohne Kontext), Matrikelnummer, beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen, Bestellungen – Warenwirtschaftssystem, Belegungslisten (Reservierungen), Auftragslisten/Auftragsformulare*	Normal bis hoch	Basis-Anforderungen sind fundamental und stets umzusetzen, sofern nicht gravierende Gründe dagegensprechen ➞ Mindestschutz.
Schutzklasse 2 (vertraulich)		**Standard-Absicherung**
Vorgänge, die aufgrund verwendeter Daten oder konkreter Verarbeitung dieser eine Aussagekraft hins. Persönlichkeit oder Lebensumstände einer Person haben, unterstützen oder zu einer solchen führen können. ➞ Die gesellschaftliche Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt („Ansehen“) *Name, Anschrift (mit Kontext), Religionszugehörigkeit, Einfache Beurteilungen von geringer Bedeutung, Zugangsdaten zu Diensten, Kommunikationsinhalte (z.B. E-Mail, Telefonat), Aufenthaltsdaten, Finanzdaten, Verkehrsdaten der Telekommunikation, Arbeitsverträge, Notenlisten, Prüfungsarbeiten, Bewerbung, Einkommen, Ordnungswidrigkeiten, Rechnungen, Geburtstagslisten, Adresslisten, Abwesenheitslisten, Urlaubskarten, Urlaubslisten, Zertifikate für Studierende, Kostenstelleneinsicht, private Telefon- & Handynummerlisten, Fotos, private Audio-/Videoaufzeichnungen, Teilnehmerlisten Studierende, Personaldaten (Benutzerantrag RZ und Homepage Lehrstuhl), Postkarten, Briefe*	Hoch bis sehr hoch	Standard-Anforderungen sind für den normalen Schutzbedarf grundsätzlich umzusetzen, sofern sie nicht durch mindestens gleichwertige Alternativen oder die bewusste Akzeptanz des Restrisikos ersetzt werden.

Schutzklasse 3 (geheim)		**Anforderungen für erhöhten Schutzbedarf**
Vorgänge, die aufgrund verwendeter Daten oder konkreter Verarbeitung dieser eine erhebliche Aussagekraft hins. Persönlichkeit oder Lebensumstände einer Person haben, unterstützen oder zu einer solchen führen können. ➞ Die gesellschaftliche Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt („Existenz“) ➞ + „Beeinträchtigung von Gesundheit, Leben, Freiheit“ *Daten, die Berufsgeheimnis unterliegen (z.B. medizinische Daten), Persönlichkeitsprofile (z.B. Bewegungsprofil) mit erheblicher Aussagekraft, Forschungs- und Entwicklungsunterlagen, dienstliche Beurteilungen, Personalakten und Nebenakten, medizinische Berichte, Schulden, Krank- und Gesundmeldungen, Zeugenschutzprogramm; Genomdaten, Anstaltsunterbringung, Straffälligkeit, Arbeitszeugnisse, Sozialdaten, Daten besonderer Kategorien nach Art. 9 DSGVO*	Sehr hoch	Anforderungen bei erhöhtem Schutzbedarf sind exemplarische Vorschläge, was bei entsprechendem Schutzbedarf zur Absicherung sinnvoll umzusetzen ist. ➞ nach Stand der Technik.

II. Quellen

Bundesamt für Sicherheit in der Informationstechnik (BSI). *Cloud Computing Grundlagen. Was ist Cloud Computing*.
URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen_node.html (Stand: 21.04.2021)

Kompetenzzentrum Trust Cloud. *Arbeitspapier – Schutzklassen in der Datenschutz-Zertifizierung.*
URL: https://tcdp.de/data/pdf/09_Arbeitspapier_Schutzklassen-in-der-Datenschutz-Zertifizierung.pdf (Stand: 21.04.2021)

Landesamt für Datenschutz (LFD) Niedersachsen. Schutzstufenkonzept.
URL: https://lfd.niedersachsen.de/download/52033/Schutzstufenkonzept_LfD_Niedersachsen_.pdf (Stand: 21.04.2021)

III. Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
bzw.	beziehungsweise
EU	Europäischen Union
EU-DSGVO	Datenschutz-Grundverordnung der Europäischen Union
etc.	et cetera
Gez.	gekennzeichnet
IT	Informationstechnik
Komm.	kommissarisch
RZ	Rechenzentrum
u.a.	unter anderen/ unter anderen
UR	Universität Regenburg

IV. Glossar

BayernShare	Der Cloud-Dienst ermöglicht ein kollaboratives Speichern, Arbeiten und Teilen von Daten und Dokumenten. Seit dem Wintersemester 2015 nutzen Studierende und Beschäftige von mittlerweile 18 Hochschulen und Universitäten in Bayern den Dienst, der zusammen vom Leibniz-Rechenzentrum (LRZ) und dem Regionalen Rechenzentrum Erlangen (RRZE) bereitgestellt wird: https://teamdrive.unibw.de/
Daten	Durch Beobachtungen, Messungen, statistische Erhebungen u. a. gewonnene [Zahlen]werte und beruhende Angaben.
Dritter	Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten.
Informationssicherheit	Übergeordnete Begriff zur Datensicherheit, der auch den Schutz und die Verfügbarkeit sonstigen geistigen Eigentums, das kein personenbezogenes Datum ist, einschließt.
Integrität	Informationen müssen während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Schutz vor unbefugten Veränderungen, Verlust und Zerstörung).
MyFiles	Eine Sync'n'Share Lösung, die vom Rechenzentrum der UR angeboten wird: https://myfiles.ur.de/filr/login
OneDrive	Microsoft OneDrive, ehemals Microsoft SkyDrive, ist ein Filehosting-Dienst von Microsoft.
Personenbezogene Daten	Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (z.B. Name, Anschrift, Geburtsdatum, familiäre Situation, Personalnummer, Beurteilungen, Fotos, berufliche Position).
Public Cloud	Im Unterschied zu einer Private Cloud stellt die Public Cloud ihre Services nicht nur einzelnen Organisationen, sondern einer Vielzahl von Anwendern über das öffentliche Internet zur Verfügung. Endnutzer können bei einem Public Cloud Dienstleister Services wie Rechenleistung, Infrastruktur, Speicherplatz oder Anwendungen mieten. Eigene Investitionen in Hard- und Software sind durch eine Public Cloud wird dadurch überflüssig.

Verantwortliche/r	Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
Verfügbarkeit	Informationen sollen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.
Vertraulichkeit	Nur Befugte dürfen Informationen zur Kenntnis nehmen können (Schutz vor unbefugtem Zugriff).

V. Dokumentenlenkung

	Version	Änderungsdatum	Autor/in
Cloud-Richtlinie.docx	1.0	27.04.2021	Elena Maria Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
öffentlich	Hauptversion	27.04.2021	Dr. Christoph Bauer

Dateiname	Version	Änderungsdatum	Autor/in
Cloud-Richtlinie.docx	0.2	22.04.2021	Elena Maria Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
öffentlich	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Cloud-Richtlinie.docx	0.1	21.04.2021	Elena Maria Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstufe	Freigabedatum	Freigabe durch
öffentlich	Entwurf	-	-

Änderungen zur vorherigen Dokumentenversion