Freie Universität Berlin

Richtlinie

zur Auslagerung von Daten in die Cloud

2. Dezember 2011

Inhalt

Steckbrief

Zielsetzung	Umgang mit Cloud-Diensten
Inhalte	Regelungen zur Speicherung von Daten in der Cloud
Zielgruppe	Alle Mitglieder der Freien Universität Berlin
Geltungsbereich	Alle dienstlichen Tätigkeiten für die Freie Universität Berlin
Gültigkeitsdauer	Unbefristet

Autoren

Mitglieder der AG IT-Sicherheit:

Hr. Camphausen (FB Mathematik u. Informatik)
Hr. Dräger (eAS)
Fr. Heinau (ZEDAT)
Fr. Pahlen-Brandt (DS)
Hr. Dr. Sommerer (FB Veterinärmedizin)
Fr. Dr. Wittkopf (FB Rechtswissenschaft)
Hr. Dr. Woidt (FB Physik)
Hr. Worch (FB Biologie, Chemie, Pharmazie)

Beraten im FIT- und CIO-Gremium und abgestimmt mit der Personalvertretung

1 Einleitung

Diese Richtlinie beinhaltet grundsätzliche Regelungen für alle Mitglieder der Freien Universität, die im Rahmen ihrer dienstlichen Tätigkeit öffentliche Cloud-Dienste (so genannte Public Clouds) zur Datenablage nutzen wollen. Sie 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 Nutzer 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 des Berliner Datenschutzgesetzes (BlnDSG). Es fordert entweder die Einwilligung der Betroffenen (im Fall der Datenverarbeitung außerhalb der EU), oder die Anwendung der Regelungen zur Auftragsdatenverarbeitung (Datenverarbeitung innerhalb der EU). Dazu sind die universitätsinternen Regelungen zu beachten, die im Handlungsleitfaden „Zugriff auf schützenswerte Daten der Freien Universität Berlin durch Externe“[1] zusammengefasst sind.

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

Sollten Sie bei der Entscheidungsfindung Beratungsbedarf haben, können Sie sich an Ihren zuständigen IT-Beauftragten wenden. (Die Liste der IT-Beauftragten ist abrufbar unter http://www.fu-berlin.de/sites/eas/it-sicherheit/downloads_zur_it-sicherheit/index.html)

[1] http://www.fu-berlin.de/sites/eas/it-sicherheit/downloads_zur_it-sicherheit/index.html

2 Geltungsbereich

Diese Richtlinie gilt für alle Mitglieder der Freien Universität Berlin, wenn sie im Rahmen dienstlicher Tätigkeiten für die Freien Universität Berlin Daten erheben, speichern oder verarbeiten.

3 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] Eckpunktepapier „Sicherheitsempfehlungen für Cloud Computing Anbieter“, BSI 2011, Art.- Nr.: BSI-Bro11/311

4 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. Der Schutzbedarf von Daten ist an der Freien Universität Berlin mittels der in der IT-Sicherheitsrichtlinie[3] festgelegten Schutzbedarfsanalyse zu bestimmen.

Hinweise auf den Schutzbedarf können zum einen aus der systematisch durchgeführten Schutzbedarfsanalyse und zum anderen aus der Datenkategorie abgeleitet werden. Daten lassen sich in die folgenden Kategorien einteilen:

Kategorie	Hinweis auf typischen Schutzbedarf
• Daten, die aus öffentlich zugänglichen Quellen stammen	keinen
• Dienstliche (nicht wissenschaftliche) Daten (z.B. aus den Bereichen Verwaltung und Lehre)	hoch bis sehr hoch
• Wissenschaftliche Daten (z.B. Untersuchungsergebnisse, Messreihen)	sehr hoch
• Wissenschaftliche Daten, sofern sie für Dritte nicht interpretierbar sind	normal bis hoch
• Personalaktendaten	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
• Daten, mit keinem oder normalen Schutzbedarf	Für die Ablage geeignet
• Daten mit hohem Schutzbedarf	Nur für die verschlüsselte Ablage geeignet
• Daten mit sehr hohem Schutzbedarf	Nicht für die Ablage geeignet
Insbesondere dürfen die folgenden Daten nicht in der Cloud abgelegt werden:	
• Personalaktendaten	Nicht für die Ablage geeignet
• Dienstliche Daten mit Personenbezug	Nicht für die Ablage geeignet
• Haushaltsdaten	Nicht für die Ablage geeignet

[3] http://www.fu-berlin.de/sites/eas/it-sicherheit/downloads_zur_it-sicherheit/index.html

5 Regelungen

Bevor Daten in der Cloud abgelegt werden, müssen die im vorangegangenen Abschnitt 4 betrachteten Abhängigkeiten zwischen der Datenkategorie, dem Schutzbedarf der Daten und der Eignung beachtet werden. Darüber hinaus gelten die in diesem Abschnitt aufgestellten Regelungen.

▪ Vorrangig Dienste der Freien Universität nutzen

Services, die von IT-Dienstleistungszentren der Freien Universität Berlin (insbesondere ZEDAT, CeDiS, eAS, UB) bereitgestellt werden, sind Cloud-Diensten externer Anbieter vorzuziehen. Nur wenn der benötigte Dienst nicht von Einrichtungen der Freien Universität bereitgestellt wird oder der bereitgestellte Dienst den Anforderungen nicht genügt, darf unter Beachtung der hier formulierten Grundsätze auf Angebote externer Anbieter zurückgegriffen werden. Die aktuell verfügbaren Dienste der universitären IT-Dienstleistungszentren können beispielsweise bei dem IT-Beauftragten der jeweiligen Einrichtung erfragt werden.

▪ 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:

- **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.

- **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 folgender Absatz) sind derartige Verfahren in der Regel bereits integriert.

- **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 Schlüssellänge und dem Schlüsselmanagement ab. Beim Einsatz von Ver-

schlüsselung 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. Wenn in sehr seltenen Fällen dennoch derartige Daten in die Cloud ausgelagert werden müssen, sind die Daten zwingend vorher zu verschlüsseln. In diesem Fall muss die Verschlüsselung inklusive des Schlüsselmanagements unter der vollständigen Kontrolle durch kompetente Stellen der Freien Universität Berlin (z.B. Hochschulrechenzentrum ZEDAT) erfolgen.

▪ 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.

▪ Dienstrechtliche Vorgaben beachten

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

▪ FU-interne Regelungen beachten

Als Ergänzung oder Konkretisierung gesetzlicher Bestimmungen und Vorschriften gilt eine Reihe von universitäts-internen Regelwerken. In erster Linie sind die Regelungen der IT-Sicherheitsrichtlinie sowie des Handlungsleitfadens „Zugriff auf schützenswerte Daten der Freien Universität Berlin durch Externe“ zu beachten. Darüber hinaus existieren weitere Leitfäden zu bestimmten Sachverhalten.[4]

▪ Sparsamer Umgang

Prinzipiell sollten bei der Nutzung entsprechender Cloud-Dienste die in Frage kommenden 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 Bereich der Freien Universität nicht verlassen dürfen. Bevor Daten auf Speichersysteme externer Anbieter ausgelagert werden, müssen erwarteter Nutzen und damit verbundene Risiken gegeneinander abgewogen werden.

[4] Die geltenden Leitfäden können unter http://www.fu-berlin.de/sites/eas/it-sicherheit/downloads_zur_it-sicherheit/ eingesehen werden.

Allgemeine Empfehlungen

Ergänzend zu den zuvor angesprochenen Themenbereichen sollten noch weitere Punkte beachtet werden:

• Cloud-Betreiber mit Firmensitz außerhalb der EU	Ein Umgang mit den Daten der Kunden gemäß den europäischen Datenschutzbestimmungen kann hier nicht vorausgesetzt werden. Insbesondere ist häufig unklar, welche Personen oder welche Stellen Zugriff auf die Daten erlangen. Für die Übermittlung personenbezogener Daten sind besondere Datenschutzvorschriften einzuhalten.
• SLA (Service-Level-Agreement) bzw. AGB (Allgemeine Geschäftsbedingungen) des Anbieters	Vor der Inanspruchnahme eines Dienstes müssen die (vertraglichen) Bedingungen, unter denen der Dienst genutzt wird, bekannt und akzeptabel sein. Hinweis: Die AGB der Anbieter können sich ändern und sollten deshalb regelmäßig überprüft werden.
• Zertifizierung des Anbieters	Wie ernst ein Anbieter die Sicherheit und den Schutz der Kundendaten nimmt, kann u.a. an dem Vorhandensein von anerkannten Prüfbescheinigungen (beispielsweise ISO 27001, entspricht BSI 100-1) abgelesen werden.

Weitere Aspekte können die Wahl des Anbieters bzw. des Cloud-Services beeinflussen (Performance, Bedienbarkeit und Handhabung der Anwendung, Kosten). Siehe hierzu Abschnitt 7.

6 Zusammenfassung

Der folgende Fragenkatalog soll bei der Eignungsprüfung des Cloud-Angebots helfen.

Sollten Sie bei der Entscheidungsfindung Beratungsbedarf haben, können Sie sich an Ihren zuständigen IT-Beauftragten wenden. (Die Liste der IT-Beauftragten ist abrufbar unter http://www.fu-berlin.de/sites/eas/it-sicherheit/downloads_zur_it-sicherheit/index.html)

1.	• Wurde das Angebot der inneruniversitären IT-Dienstleister (insbesondere ZEDAT CeDiS, eAS, UB) geprüft? • Ist ein FU-Service zur Ablage der Daten geeignet?
2.	• Wurden die SLA (Service-Level-Agreement) bzw. AGB (Allgemeine Geschäftsbedingungen) des Anbieters angesehen? • Passen die Bedingungen des Anbieters zu den Anforderungen?
3.	• Erfüllt der Cloud-Dienst die Anforderungen an die Verfügbarkeit der Daten?
4.	• Erfüllt der Cloud-Dienst die Anforderungen an die Integrität der Daten? • Wurden Vorkehrungen getroffen, hohe Integritätsanforderungen zu erfüllen?
5.	• Gestatten die Anforderungen hinsichtlich der Vertraulichkeit der Daten eine unverschlüsselte Ablage in der Cloud?
6.	Wenn die Anforderungen hinsichtlich der Vertraulichkeit der Daten nur eine *verschlüsselte* Ablage in der Cloud erlauben: • Wird die Verschlüsselung vor der Abspeicherung durchgeführt? • Werden die Schlüssel im Bereich der Freien Universität Berlin abgelegt?
7.	Wenn *personenbezogene* Daten in der Cloud abgelegt werden sollen: • Dienstliche personenbezogene Daten dürfen nicht in der Cloud abgelegt werden. • Wurde geprüft, ob alle datenschutzrechtlichen Anforderungen, insbesondere hinsichtlich der Auftragsdatenverarbeitung, erfüllt sind?
8.	• Wurde geprüft, ob gesetzliche oder andere Vorschriften die Ablage der Daten auf Systemen außerhalb der Freien Universität Berlin erlauben?
9.	• Wurde geprüft, ob die Daten bestimmten Löschfristen unterliegen? • Genügen die vom Cloud-Dienstanbieter bereit gestellten Dienste diesen Anforderungen?

7 Weiterführende Dokumente zu Cloud Computing

- **Cloud Computing und Datenschutz**
  Thilo Weichert, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
  https://www.datenschutzzentrum.de/cloud-computing/

- **Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien**
  der Konferenz der Datenschutzbeauftragten des Bundes und der Länder,
  Version 1.0, Stand 26.09.2011,
  http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

- **Sichere Internet-Dienste – Sicheres Cloud Computing für Mittelstand und öffentlichen Sektor (Trusted Cloud)**
  Bundesministeriums für Wirtschaft und Technologie,
  http://www.trusted-cloud.de/

- **Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter**
  Bundesamt für Sicherheit in der Informationstechnik (BSI),
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile