Hochschule Magdeburg • Stendal

IT-Sicherheitsmanagementteam (SMT)

# Richtlinie

# zur Auslagerung von Daten in die Cloud [1]

Fassung: 6.8.2013

[1] Die Richtlinie basiert auf einem gleichnamigen Papier der FU Berlin, dass uns dankeswerter Weise zur Nutzung zur Verfügung gestellt wurde.

## 1 Einleitung

Diese Richtlinie beinhaltet grundsätzliche Regelungen für alle Mitglieder der Hochschule Magdeburg-Stendal, 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 Datenschutzgesetzes des Landes Sachsen-Anhalt. 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).

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, sollten Sie sich an Ihren zuständigen IT-Sicherheitsbeauftragten im Fachbereich wenden.

## 2 Geltungsbereich

Diese Richtlinie gilt für alle Mitglieder und Angehörigen der Hochschule Magdeburg-Stendal, wenn sie im Rahmen dienstlicher Tätigkeiten für die Hochschule Magdeburg-Stendal 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]

Die vorliegende 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**. Hinweise zu Schutzbedarfsanalyse und Beispiel finden Sie in der **Anlage1** dieser Richtlinie.

Hinweise auf den Schutzbedarf können zum einen aus der systematisch durchgeführten Schutzbedarfsanalyse und zum anderen aus der Datenkategorie abgeleitet werden.

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).

Daten lassen sich in die folgenden Kategorien einteilen:

| Kategorie | Typischer Schutzbedarf |
|---|---|
| Daten aus öffentlichen Quellen | keinen |
| Dienstliche (nichtwissenschaftliche, ohne Personenbezug) Daten aus Lehre und Verwaltung, | hoch bis sehr hoch* |
| Wissenschaftliche Daten (Untersuchungsergebnisse, Messreihen,...) | sehr hoch |
| Sonstige wissenschaftliche Daten, sofern für Dritte nicht interpretierbar | normal bis hoch* |
| Personalunterlagen und personenbezogene Daten | sehr hoch |

*vom Eigentümer der Daten abzuwägen

Ein Schutzbedarf wird grundsätzlich hinsichtlich der drei Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit differenziert bestimmt (siehe auch Anlage 1). 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 normalem Schutzbedarf | Für die Ablage geeignet |
| Daten mit hohem Schutzbedarf | NICHT für die Ablage empfohlen und wenn dann Nur VERSCHLÜSSELT (s.a. Hinweis zu Pkt 5) |
| Daten mit sehr hohem Schutzbedarf | Dürfen NICHT abgelegt werden |

**Besonders folgende Daten dürfen NICHT in der Cloud abgelegt werden:**

A) **PERSONALUNTERLAGEN UND PERSONENBEZOGENE DATEN**
B) **DIENSTLICHE DATEN MIT PERSONENBEZUG**
C) **INTERNE HAUSHALTSDATEN**

Hochschule
Magdeburg • Stendal

## 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 IT-Dienste der Hochschule Magdeburg-Stendal nutzen**
  Services, die von IT-Dienstleistungszentren der Hochschule – ZKI, BiBo - bereitgestellt werden, sind externen Cloud-Diensten vorzuziehen. Das ZKI bietet persönliche Homeverzeichnisse für alle Mitglieder der Hochschule. Diese kann man so einrichten, dass sie über den Dateimanager in egroupware weltweit erreichbar wären. Dieser Zugriff ist Cloud-Mechanismen gleich zu setzen, darf also z.Bsp. NICHT für die Ablage personenbezogener Daten benutzt werden.

  Nur wenn der benötigte Dienst nicht von diesen Einrichtungen der Hochschule bereitgestellt wird oder der bereitgestellte Dienst den Anforderungen nicht genügt, darf unter Beachtung der in der vorliegenden Richtlinie formulierten Grundsätze auf Angebote externer Anbieter zurückgegriffen 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 der Einsatz eines Datenverschlüsselungssystems zwingend notwendig. Viele Anbieter von Speicherplatz in der Cloud bieten Dienste zur Datenverschlüsselung. Beachten sie dabei, dass diese Verschlüsselungsdienste oft nicht zuverlässig nachvollziehbar sind (wer hat Zugriff auf die Schlüssel und damit auf die Daten). Dieser Verschlüsselungsweg wird nicht empfohlen.

  Die Verschlüsselung soll 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 Verschlüsselung muss darauf geachtet werden, dass sie nach allgemein anerkannten Regeln als sicher gilt. Das BSI (Bundesamt für Sicherheit in der IT) empfiehlt z.Bsp. die OpenSource-Anwendung „7-Zip".
  ( https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Datenverschluesselung/Praxis/Software/software_node.html

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

- **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.

- **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 Hochschule nicht verlassen dürfen.
  Bevor Daten auf Speichersysteme externer Anbieter ausgelagert werden, müssen erwarteter Nutzen und damit verbundene Risiken gegeneinander abgewogen werden.

- **Dienstrechtliche Vorgaben und HS-interne Regelungen 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 Hochschule abgelegt werden. Inwieweit bei der Datenspeicherung dienstrechtlich Vorschriften zu beachten sind, muss im Zweifel unter Einbeziehung des jeweiligen Vorgesetzten geklärt werden.
  Als Ergänzung oder Konkretisierung gesetzlicher Bestimmungen und Vorschriften gilt eine Reihe von hochschulinternen Regelwerken. In erster Linie sind die Regelungen der IT-Ordnung und der IT-Sicherheitsrichtlinie zu beachten.

- **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. 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.

## 6 Zusammenfassung

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

Bei Fragen wenden Sie sich bitte an ihren zuständigen IT-Sicherheitsbeauftragten im Fachbereich.

| | |
|---|---|
| 1. | ☐ Wurde das Angebot der HS-internen IT-Dienstleister (insbesondere ZKI und BiBo) geprüft?<br>☐ Ist ein HS-Service zur Ablage der Daten geeignet? |
| 2. | ☐ Wurden die SLA (Service-Level-Agreement) bzw. AGB (Allgemeine Geschäftsbedingungen) des Anbieters angesehen?<br>☐ 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?<br>☐ 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:<br>☐ Wird die Verschlüsselung vor der Abspeicherung durchgeführt?<br>☐ Werden die Schlüssel im Bereich der Hochschule abgelegt? |
| 7. | Wenn *personenbezogene* Daten in der Cloud abgelegt werden sollen:<br>☐ **Dienstliche personenbezogene Daten dürfen nicht in der Cloud abgelegt werden**.<br>☐ 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 Hochschule Magdeburg-Stendal erlauben? |
| 9. | ☐ Wurde geprüft, ob die Daten bestimmten Löschfristen unterliegen?<br>☐ Genügen die vom Cloud-Dienstanbieter bereit gestellten Dienste diesen Anforderungen? |

Hochschule
Magdeburg • Stendal

## 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

- **On the Security of Cloud Storage Services**, Studie der Frauenhofer-SIT
https://www.sit.fraunhofer.de/de/angebote/projekte/cloud-studie/

Der Kanzler

**Anlage 1**

**Hinweise für die Festlegung des Schutzbedarfs von Daten**

Die zu schützenden Daten sind zu identifizieren, zu analysieren und zu dokumentieren.

Der Schutzbedarf wird über die Abschätzung der schlimmsten denkbaren Folgen des Verlustes von
A) der Vertraulichkeit,
B) der Integrität und
C) der Verfügbarkeit von Daten ermittelt.

Die Abschätzung hat gesondert für folgende Schadenskategorien zu erfolgen:
•Beeinträchtigung des informationellen Selbstbestimmungsrechts
•Beeinträchtigung der persönlichen Unversehrtheit
•Beeinträchtigung der Aufgabenerfüllung
•Negative Außenwirkung
•Finanzielle Auswirkungen
•Verstoß gegen Gesetze, Vorschriften und Verträge

BEISPIELE:
Daten/Datenkategorien
1. Name (Vorname, Nachname)
2. Adresse (Straße mit Hausnummer, Postleitzahl und Ort)
3. Fachbereichszugehörigkeit
4. Studiengang
5. Prüfungsergebnisse
6. Belegte Veranstaltungen

Vertraulichkeit
**Angenommen, Unbefugte erlangen Kenntnis von den Personaldaten->**
Welche Folgen hätte diese Verletzung des informationellen Selbstbestimmungsrechts im schlimmsten Falle?
□Der Umgang mit Kollegen kann beeinträchtigt werden. Der berufliche Werdegang kann erheblich beeinträchtigt werden.

Welche Folgen hätte dies im schlimmsten Falle für die persönliche Unversehrtheit?
□Keine, Folgen für die Gesundheit können ausgeschlossen werden.

Welche Folgen aus Vorschriften/ Gesetzen entstehen?
□Das Datenschutzgesetz des Landes Sachsen-Anhalt wird verletzt!
(...)
Beispiel Integrität:
**Angenommen, Forschungsdaten werden unbefugt verändert->**
Welche negativen Außenwirkung hätte dies im schlimmsten Falle?
□Die Hochschule Magdeburg-Stendal würde als unzuverlässige Organisation angesehen werden. Es muss von einem überregionalen (bundesweiten) Ansehensverlust ausgegangen werden.
(...)
Beispiel Verfügbarkeit:
**Angenommen, die Daten von Studierenden stehen nicht zur Verfügung->**
Welche Auswirkungen auf die Aufgabenerfüllung hätte dies im schlimmsten Falle?
□Prüfungen können nicht sachgemäß durchgeführt werden. Rückmeldungen sind nicht möglich. Regressforderungen können möglich sein.
(...)