Freie Universität Berlin

Guidelines for Storing Data

in Cloud Data Systems

2-Dec-2011

Contents

Summary

Purpose	Treatment of cloud services
Contents	Principles for storing data in cloud systems
Target audience	All members of Freie Universität Berlin
Applies to	All work activities within Freie Universität Berlin
Validity period	Unlimited

Authors

Members of the working group for IT security:

Hr. Camphausen (Dept. of Math and Comp. Sci.)

Hr. Dräger (eAS)

Fr. Heinau (ZEDAT)

Fr. Pahlen-Brandt (Data Privacy)

Hr. Dr. Sommerer (Dept. of Vet. Medicine)

Fr. Dr. Wittkopf (Dept. of Law)

Hr. Dr. Woidt (Dept. of Physics)

Hr. Worch (Dept. Biology, Chem., Pharmacy)

Consultation with the FIT and CIO boards, and coordinated with the employee representative.

1 Introduction

These guidelines contain fundamental provisions for all members of Freie Universität Berlin who wish to use public cloud services (so-called Public Clouds) for storing data in the scope of their work activities. The document discusses general risks and assists in clarifying in which cases or under which conditions cloud services may be used.

Particular dangers threaten when data is stored or processed with assistance of cloud services. In particular, the dynamic distribution of memory capacities across various locations, which as a rule are not known to the user, require specific preparations with regard to information security and data protection.

The provisions of Berlin's Data Protection Law (BlnDSG) apply to processing personal data in cloud systems. This requires either the approval by the affected parties (in case of data processing outside of the EU), or the application of guidelines for commissioned data processing (data processing within the EU). In addition, the university-internal guidelines are to be observed, which are summarized in the management guideline "Access by Third Parties to Sensitive Data at Freie Universität Berlin"[1].

In private surroundings, cloud services are frequently used with relative little care. In view of the situation of the disappearing boundaries between private and work requirements, especially in the field of IT, these guidelines will help to call attention to the potential risks and to offer corresponding management directives.

If you need advice to make a decision, you may contact the IT representative responsible for your department (the list of IT representatives may be found under:
http://www.fu-berlin.de/sites/it-sicherheit/downloads).

[1] http://www.fu-berlin.de/sites/it-sicherheit/downloads

2 Scope of Applicability

These guidelines apply to all members of Freie Universität Berlin, whenever they collect, save, or process data for the Freie Universität in the scope of their work activities.

3 Distinctions and Definitions of Terms

IT services that can be used via a data or communications network independently of location and time, are generally designated as “cloud computing” systems. However, there are various slightly different definitions of the term. For the following discussion, our definition of the term is derived from a definition established by the (German) Federal Office for Information Security (BSI) for the term “cloud computing” (and translated here):

> *Cloud Computing designates the dynamic provision, use, and billing of IT services via a network, adapted to demand. As a rule, these IT services may be used independently of location and time, with the assistance of all common IT devices. The IT infrastructure provided remains hidden from the user.*[2]

These guidelines consider aspects of data storage, thus the temporary or long-term allocation of data to external (third party) service providers, using the assistance of cloud services. Additional cloud services, such as managerial or computational services, are not discussed here.

[2] Whitepaper “Security Recommendations for Cloud Computing Providers”, BSI 2011, Art.- Nr.: BSI-Bro11/311

4 Data Categories and Suitability for Cloud Usage

To decide under which conditions data storage in cloud systems is acceptable, the confidentiality of the data represents a fundamental guideline. The security requirement for data at Freie Universität Berlin is to be determined by means of the security analysis established in the IT Security Guideline.[3]

Indications of the security requirement may be derived first by a systematically performed security requirement analysis, and secondly from the category of the data. Data may be organized into the following categories:

Data category	Typical security requirement
• Data from publicly available sources	none
• Official work-related (not scientific) data (such as instructional or administrative data)	high to very high
• Scientific data (such as research results, or measurement data)	very high
• Scientific data, provided it is not interpretable by third parties	normal to high
• Personnel file data	very high

The following aspects are to be observed in all cases:

- Data protection specifications apply to all personal data (in both work and in private connections).
- Data without a personal connection may also have a very high security requirement (for example, due to non-disclosure agreements).

The security requirement is determined fundamentally with regard to three security goals: availability, integrity, and confidentiality. Measures to ensure the safety of the data must be implemented accordingly. These security requirements for data lead inevitably to the suitability (or non-suitability) for storing the data in cloud systems:

Security level	Suitability for cloud storage
• Data having no or normal security requirements	Suitable for storage
• Data with high security requirements	Suitable only for storage of encrypted data
• Data with very high security requirements	Not suitable for storage
In particular, the following data cannot be stored in cloud systems at all:	
• Personnel file data	Not suitable for storage
• Official data with personal references	Not suitable for storage
• Budgetary data	Not suitable for storage

[3] http://www.fu-berlin.de/sites/it-sicherheit/downloads

5 Provisions

Before data is stored in cloud systems, the dependencies described above in Section 4 between the category of the data, the protection required by the data, and suitability for storage must be considered. In addition, the provisions listed in this Section also apply:

Prefer the use of Freie Universität services

Services provided by IT service centers at Freie Universität Berlin (in particular ZEDAT, CeDiS, eAS, UB) are to be preferred over cloud services from external providers. Only when the services needed are not offered by facilities of the Freie Universität, or when the services available do not satisfy the requirements, may offerings from external providers be considered, under consideration of the principles formulated here. The services currently available from the university's IT service centers may be obtained by contacting the IT representative of each respective department.

The protection level required by the data governs the extent of cloud use

The level of protection required by the data intended to be stored governs not just whether storage is permitted, but also under which conditions this may occur. The protection requirement is to be considered separately according to the three security goals: availability, integrity, and confidentiality:

Availability

It is necessary to check in advance what claims the provider of the cloud services makes with regard to availability. If very high requirements are placed on availability, then data storage in the cloud system can only be considered when the provider of the cloud services guarantees very high availability.

Integrity

The integrity of the data (protection against unauthorized tampering) is not generally guaranteed by cloud storage providers. If high or even very high requirements are specified in this regard, the user must undertake suitable measures on his or her own initiative to guarantee integrity of the data. For example, checksums may be used that permit detection of any alterations to the data. Such processes are usually already integrated in systems for data encryption (see the following paragraph).

Confidentiality

When *high requirements* are placed upon confidentiality, the use of an encryption system is absolutely required. Many providers of storage space in cloud systems also offer data encryption services. When using these encryption services, it is generally not possible to reliably verify who has access to the (encryption) key, and therefore has (potential) access to the data. Access to the key by the service provider must be prevented. For this reason, the encryption itself should be performed *before* the data is transferred into the cloud system. Among other things, the security of the encrypted data depends on the quality of the encryption algorithm, the encryption software, the length of the key, and the management of the key. When using encryption, it must be considered whether it is safe according to commonly recognized rules.

Cloud storage systems should generally be avoided for data with *very high* *requirements* on confidentiality. However, if in very rare cases such data must nevertheless be stored in a cloud system, the data must absolutely be encrypted in advance. In this case, the encryption, including the management of the keys, must occur under complete control of responsible facilities of Freie Universität Berlin (for example, ZEDAT computing services).

- ### Deleting (erasing) data

  Providers of cloud storage normally employ storage techniques that permit efficient utilization of the physical memory capacity. This memory management may mean that data is often (actually) deleted only after a certain period of time. In principle, it is not possible to exclude that execution of the deletion command simply suppresses the data for the user, but does not actually delete it. For this reason, data that is (for example) subject to legal requirements for deletion is not suitable for storage in cloud systems.

- ### Observe work-related regulations

  For administrative data in particular (and above all for personnel and budgetary data) there are often detailed regulations about how this data is to be handled. For example, various regulations provide that personnel files may not be freely removed from the personnel department. Therefore, such personal data is also not to be stored in memory outside Freie Universität Berlin. To which extent work-related rules must be considered in storing data, must in case of doubt be clarified with each of the appropriate authorities.

- ### Observe internal FU regulations

  A series of internal university guidelines serve as enhancements or concrete guides to legal provisions and regulations. First and foremost, the provisions of the IT Security Guidelines, as well as the management guideline “Access by Third Parties to Sensitive Data at Freie Universität Berlin” are to be observed. In addition, there are additional guidelines for specific issues.[4]

- ### Limited use

  When using appropriate cloud services, the potential amount of data should in principle be limited to the minimum needed. For example, when transferring entire directory trees into a cloud system, it is easy to overlook that a sub-directory may contain sensitive data that is not allowed to leave the confines of Freie Universität. Before data is transferred to memory systems of external providers, the expected benefits and the concurrent risks must be weighed against one another.

[4] The corresponding guidelines may be reviewed at: http://www.fu-berlin.de/sites/it-sicherheit/downloads

General recommendations

In addition to the issues discussed above, the following points should also be considered:

- Cloud providers with headquarters outside the EU

  Management of the customer’s data in accordance with European data protection provisions cannot be presumed here. In particular, it is frequently unclear which individuals or locations will have access to the data. Special data protection regulations are to be observed for the transfer of personal data.

- The provider’s Service Level Agreement (SLA) or General Business Terms and Conditions *(German: “AGB”)*

  Before ordering a service, the contractual conditions under which the service will be used must be fully known and acceptable.
  Please note: The provider’s “general terms” may change without prior notice, and therefore should be verified on a regular basis.

- Certification of the provider

  The degree to which a provider takes security and protection of the customer’s data seriously can be indicated by the presence of recognized certifications (for example, ISO 27001, corresponds to BSI 100-1).

Additional aspects may influence the selection of a cloud service provider (performance, usability and serviceability of the application, costs). See also Section 7.

6 Summary

The following catalog of questions is intended to help examine the suitability of cloud services.

If you need advice to make a decision, you may contact the IT representative responsible for your department (the list of IT representatives may be found under: http://www.fu-berlin.de/sites/it-sicherheit/downloads).

1.	• Have the services offered by internal university IT service providers been checked? (In particular: ZEDAT CeDiS, eAS, UB) • Is there an FU service that is suitable to store the data?
2.	• Have the provider's Service Level Agreements (SLA) and/or general business terms and conditions *(AGB)* been reviewed? • Do the provider's conditions satisfy the requirements?
3.	• Does the cloud service fulfill the requirements for availability of the data?
4.	• Does the cloud service fulfill the requirements for data integrity? • Have measures been taken to ensure high integrity requirements?
5.	• Do the requirements for data confidentiality permit unencrypted storage in a cloud system?
6.	If the data confidentiality requirements permit only *encrypted* storage in a cloud system: • Will be the encryption be performed before storage? • Are the keys stored at Freie Universität Berlin?
7.	If *personal* data is to be stored in a cloud system: • Work-related data with personal identification may *not* be stored in a cloud system. • Has it been checked whether all data protection requirements have been fulfilled, in particular with regard to contractual data processing?
8.	• Has it been verified whether laws or other regulations permit storage of the data in systems outside of Freie Universität Berlin?
9.	• Is the data subject to deletion after specific periods of time? • Do the services offered by the cloud service provider fulfill these requirements?

7 Further documentation about cloud computing

- **Cloud computing and data privacy**
  Thilo Weichert, Independent Center for Data Protection for the German State of Schleswig-Holstein, Article Number: BSI-Bro11/314e
  https://www.datenschutzzentrum.de/cloud-computing/
  (This document is available both in English and German.)

- **Orientation to Cloud Computing by the working groups on Technology and Media**
  Conference of data protection representatives of the German Federal and State Governments, version 1.0, dated: 26-Sep-2011,
  http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf
  (This document is only available in German.)

- **Flyer: Trusted Cloud - Safe Cloud Computing for Public and Business Sectors**
  German Federal Ministry for Business and Technology, dated: Feb-2014
  http://www.trusted-cloud.de/
  (All documents from this site are only available in German.)

- **White Paper - Security Recommendations for Cloud Computing Providers**
  (German) Federal Office for Information Security (BSI), dated: 22-Jun-2011
  https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile
  (BSI offers this document both in English and German, under separate addresses.)