Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Sync & Share Policy

Version 1.0

22 August 2016

Introduction

This policy contains the basic regulations that apply for all members of Universität Hamburg, who use Sync & Share services for data storage, data synchronization, and collaborative sharing as part of their official duties. It informs on the general risks and helps clarify in which cases and under which conditions Sync & Share services can be used.

Special risks arise when Sync & Share services are used to store or process (personal) data. Particularly the dynamic distribution of storage capacities, potentially across different locations that are generally unknown to users, calls for special precautions (relating to information security and data protection).

The processing of personal data in Sync & Share services is subject to the provisions of the Hamburg data protection and privacy act (HmbDSG). It requires either the consent of the data subjects (in the case of data processing outside the EU) or application of the regulations on commissioned data processing (in the case of data processing within the EU). Additionally, University-internal regulations (e.g., service agreements) must be observed.

In the private sphere, Sync & Share services are often used relatively carelessly. Against the backdrop of the increased blurring between private and business matters (especially in IT settings), this policy aims to help draw attention to potential risks and to provide appropriate instructions.

This document is based on the policy on outsourcing data to the cloud published by Freie Universität Berlin.[1]

[1] AG IT-Sicherheit, Freie Universität Berlin, Kaiserswerther Str. 16/18, 14195 Berlin, Richtlinie zur Auslagerung von Daten in die Cloud, 2 December 2011. www.mi.fu-berlin.de/wiki/pub/IT/ItProcess/Richtlinie_Cloud-Datenablage_-_1_0.pdf

1 Scope

This policy applies to all members of Universität Hamburg who collect, store, share, synchronize, or process data on various devices in the course of their official activities for Universität Hamburg.

2 Definitions

In this policy, file services and services for data synchronization and cooperative sharing that can be used independently of time and place via a communication network are referred to collectively as "Sync & Share services."

> *Sync & Share describes the dynamic needs-based provision, use, and invoicing of file services via a network. As a rule, such file services can be used independently of time and place via all standard IT devices. The IT infrastructure provided remains hidden from users. Furthermore, data can be shared with other people across organizations, e.g., to cooperate on joint projects. Sync & Share enables the synchronization of data on different device classes.*

This policy considers aspects of data storage, that is to say, the short- or longer-term transfer of data to internal or external service providers using Sync & Share services.

3 Data categories and their suitability for the use of Sync & Share services

The basic principle for deciding under which conditions data can be outsourced to a Sync & Share service is the data protection requirement.

Indications of the protection requirement can be derived from a systematic analysis of the protection requirement on the one hand and the data category on the other. Data can be divided into the following categories:

Category	**Typical protection requirement**
Data obtained from publicly accessible sources	None
Official (non-scientific) data (e.g., from administration and teaching)	High to very high
Scientific data (e.g., research results, measurements)	Normal to very high
Data in personnel files	Very high
Private data (e.g., friends' contact details)	Normal to very high

The following aspects must be considered in each case:

- The data protection legislation applies to all personal data (whether it relates to business or private matters).
- Even data without a personal reference can have a very high protection requirement (e.g., due to confidentiality agreements).

The protection requirement is generally determined according to the three protection goals of **availability**, **integrity**, and **confidentiality**. Differentiated precautions must then be taken to ensure data security. The (un)suitability for storage within Sync & Share services derives from the data's protection requirement:

Protection requirement	**Suitability for storage**
Data with no or a normal protection requirement	Yes
Data with a high protection requirement	Encrypted, when technically feasible
Data with a very high protection requirement	No

4 Regulations

Before a Sync & Share service can be used to store data, the data category, the data's protection requirement, and the suitability determined in Section 3 must be reviewed. The rules detailed in this section additionally apply.

(1) Use Sync & Share services sparingly

When using Sync & Share services, the data volumes should in principle be limited to the necessary minimum. For example, when transferring entire directory trees to a Sync & Share service, it can easily be overlooked that sensitive data that must not leave Universität Hamburg's network has been stored in a subdirectory. Before data is outsourced to the storage systems of external providers, the anticipated benefits and associated risks must be weighed up.

(2) Use the services offered by Universität Hamburg

Wherever possible, the basic services provided by the RRZ must be used: UHHShare (Sync & Share service, "Dropbox alternative"), UHHDisk (file services via the internet or network drives), and SharePoint (cooperative communication and information platform, portal). These can be used without restriction for data up to the protection level of "High."

Only if the required service is not provided by the RRZ or other institutions of Universität Hamburg or if the service provided does not meet the requirements can external providers be used, subject to the principles set out here and following the appropriate consultation with the RRZ.

(3) The protection requirement determines the scope of Sync & Share usage

The protection requirement of the data to be outsourced not only determines whether outsourcing is permissible, but also the conditions under which it can take place. The protection requirement must be considered separately according to the three protection goals of availability, integrity, and confidentiality:

(3.1) Availability

The statements made by the provider of the Sync & Share service about availability must be checked beforehand. If very high requirements exist for the availability of data, storage in a Sync & Share service is only an option if the provider of the Sync & Share service guarantees very high availability.

(3.2) Integrity

Providers of Sync & Share services generally do not guarantee the integrity of data. If high or even very high requirements exist for the integrity of data, the user must take appropriate measures for themselves to ensure the integrity. Checksums can be used to detect changes to the data, for example. Such procedures are usually already integrated into data encryption systems (see next paragraph).

(3.3) Confidentiality

If high requirements exist for the confidentiality of data, the use of a data encryption system is absolutely essential as an adequate measure. Many providers of Sync & Share storage services also offer data encryption services. However, as a rule it is not possible to reliably trace who has access to the keys (and thus to the data) when using these encryption services. It must not be possible for the service provider to access the keys. Hence Sync & Share service users should encrypt the data themselves before they transfer it. The security of encrypted data among others depends on the quality of the encryption algorithm, the encryption software, the key length, and the key management. When using encryption, it must be verified that it is considered secure according to the generally recognized rules. Generally speaking, Sync & Share services should not be used to store data for which very high confidentiality requirements exist. If such data must be outsourced to a Sync & Share service (in very rare cases), the data must be encrypted beforehand. In this case, encryption, including key management, must take place under the full control of competent bodies at Universität Hamburg (e.g., the RRZ).

(4) Data deletion

Providers of Sync & Share services normally use storage technology to make efficient use of physical storage capacities (deduplication). As a consequence, data can often only be deleted after a certain period of time.
In principle, it cannot be ruled out that data is only hidden from the user but not deleted when the delete command is sent. Hence data that is subject to a legal obligation of deletion is unsuitable for storage in Sync & Share services, for example.

(5) Observe civil service legislation

Especially for administrative data (particularly personnel, budget, and financial data), detailed regulations often exist on how this data should be handled. Various regulations stipulate that personnel files cannot simply leave the HR department, for example. This means that such personal data cannot be stored outside Universität Hamburg or the Free and Hanseatic City of Hamburg. In case of doubt, University members must clarify with their respective superior the extent to which employment law regulations must be observed when storing data.

(6) Observe Universität Hamburg's regulations

A number of University-internal regulations (e.g., the password policy, user regulations, etc.) supplement or further specify legal provisions and regulations.

(7) General recommendations

In addition to the aspects mentioned above, a number of other points must be borne in mind:

Sync & Share service providers based outside the EU: It cannot be assumed here that client data will be handled in accordance with the European data protection regulations. Specifically, it is often unclear which persons or bodies have access to the data. Special data protection regulations must be observed for the transfer of personal data.

Service level agreement (SLA) or general terms and conditions (GTC) of the provider: The (contractual) conditions for the use of a service must be known beforehand and be acceptable.

Certification of the provider: How seriously a provider takes the security and protection of customer data can for example be seen from the recognized test certificates that exist (e.g., ISO 27001, equivalent to BSI 100-1).

5 Checklist and questionnaire

Use the following questions to determine the suitability of Sync & Share services.

1 *Review the internal options*

- Have the options offered by Universität Hamburg's IT service provider (RRZ) been checked?
- Is a service offered by Universität Hamburg suitable for storing the data?

2 *Review the external provider's contractual conditions*

- Have the provider's service level agreements (SLA) or general terms and conditions (GTC) been checked?
- Do the provider's conditions meet the requirements?

3 *Review availability*

- Does the Sync & Share service meet the data availability requirements?

4 *Review integrity*

- Does the Sync & Share service meet the data integrity requirements?
- Have precautions been taken to meet high integrity requirements?

5 *Unencrypted storage*

- Do the data confidentiality requirements permit unencrypted storage in an external Sync & Share service?

6 *Encrypted storage*

If the data confidentiality requirements allow encrypted storage in an external Sync & Share service only:

- Is the encryption carried out prior to storage?
- Are the keys stored exclusively at Universität Hamburg?

7 *Personal relevance*

If personal data is to be stored in a Sync & Share service:

- Has it been checked whether all data protection requirements (in particular with regard to commissioned data processing) have been met?

8 *Compliance with the regulations*

- Has it been checked whether legal/other requirements permit the storage of data on systems outside Universität Hamburg?

9 *Deletion*

- Has it been checked whether the data is subject to legally-binding deletion periods?
- Do the Sync & Share provider's services meet these requirements?