Goethe University recommendations and best practices for outsourcing data to the cloud

The following recommendations apply to all members of Goethe University Frankfurt. They regulate the official use of cloud services. Goethe University regulations and statutes, in particular IT security regulations, IT security guidelines and the IuK use regulation[1], are not affected by these recommendations.

Against the background of the increasingly dissolving separation between personal and professional concerns, particularly in the IT environment, this guidelines is intended to help raise awareness regarding potential risks and provide corresponding recommendations for action.

Consciously or unconsciously, cloud services have been being used in many areas for many years. It should be noted that most of these "free" services are "paid for" with the data of their users. This can sometimes lead to the assignment of rights for the data stored in cloud storage. For this reason, the storing of data in public clouds should be avoided.

Goethe University's Security Management Team (SMT) recommends the following rules when storing data in the cloud:

1) The Sync & Share Solution **Hessenbox** (https://hessenbox.uni-frankfurt.de) is recommended as cloud service for the online storage of files. It is operated by Goethe University and provided at no cost. Hessenbox is registered as an approved IT procedure. You can find more information (in German) at this link:
https://www.rz.uni-frankfurt.de/hessenbox

2) Data stored in Hessenbox must be encrypted by the data owner **depending on protection needs**. The following tools may be used and are available at no cost:

   - **Files in a file**
     7-Zip (https://www.7-zip.org/)

   - **Files in a container**
     VeraCrypt (https://www.veracrypt.fr/en/Home.html)
     Cryptomator (https://cryptomator.org/de/)

[1] Allgemeine Nutzungsordnung für die Informationsverarbeitungs- und Kommunikationsinfrastruktur der Goethe-Universität Frankfurt – General use regulations for information processing and communication infrastructure at Goethe University Frankfurt

3) For security reasons, we recommend only using cloud services via their websites and to avoid apps and other programmes. If the use of apps or other programmes cannot be avoided for the synchronising of data, make sure that only the **required directories** are synchronised.

4) Of course, it is also important to pay close attention to the group of people to whom the data is **released**.

5) Cloud services such as Dropbox, Google Drive, iCloud, OneDrive, Amazon Drive etc. should only be used **if absolutely unavoidable**. The following points should be heeded:

   - The official use of external cloud services have to be approved by Goethe University's official **data security officer** (dsb@uni-frankfurt.de).

   - The use of external cloud services for personalised or copyright-protected material is **prohibited**.

   - **Confidentiality** can **not be guaranteed** with regard to external providers. Data should therefore be encrypted before being stored with external providers.

6) Please contact your IT support or your IT security officer if you have any questions.

Further information:

- Bundesamt für Sicherheit in der Informationstechnik (BSI) - (Federal Office for Information Security)
  https://www.bsi-fuer-buerger.de

- DFN Computer Emergency Response Team (DFN-CERT)
  https://www.dfn-cert.de

- IT-Sicherheitsmanagement-Team (SMT) - Goethe University IT Security Management Team
  https://www.uni-frankfurt.de/smt

- Goethe University Computer Emergency Response Team (GU-CERT)
  https://www.rz.uni-frankfurt.de/gu-cert

- Hochschulrechenzentrum (HRZ) – Goethe University Computing Centre
  https://www.uni-frankfurt.de/hrz/it-sicherheit