Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Rules for the use of external cloud services managed by IT Services

If you use such cloud services (e.g. Microsoft 365, Zoom, Google Workspace), there are special, i.e. cloud-specific risks for your data.

To protect your data, the following rules apply:

1) External cloud services may be used for confidential data if they appear in the release list for users and the information owner* agrees. If in doubt, contact the information owner.
2) If you use **additional services** such as add-ins, translation services, literature management, etc., which are not included in the release list, you must not process or store confidential, strictly confidential or personal data in such services.

* *Information owners are responsible for the data that is collected and processed on their behalf. They therefore decide how much their data should be protected (through confidentiality classification) and whether it can be outsourced to external cloud services. Information owners can be: heads of organisational units (e.g. heads of departments and staff, professors).*

This means:

- If you use (upload, comment, share in a cloud service) data that someone else has created, follow the instructions of that other person. If you are not sure, ask the person concerned about the classification status.
- In the first instance, ask the information owner how the data should be classified and used.
- If no information owner is known within ETH, ask the originator/author.

Cloud-specific risks are namely the following:

- Some dependence on the cloud provider, e.g. for availability and service quality
- Possible loss of data or control by the cloud provider
- Possibly complicated, inconsistent or contradictory terms and conditions and data protection provisions on the part of the cloud provider.
- Possibly unfavourable or missing liability regulations in the event of a claim
- Even data encryption offers only limited protection
- If the cloud provider is taken over or the service is discontinued, transferring the data back to ETH can become a problem.
- Cloud providers can be obliged by their government to disclose data ("lawful access"; especially in the United States)
- Cloud services are becoming increasingly attractive for cyberattacks and (industrial) espionage

When working with external cloud services, it is important for ETH Zurich to maintain access to and control over its data at all times.

Please also ensure that you do not infringe any third-party rights, in particular data protection and copyright, when processing data in external cloud services.

Comments on the e-mail infrastructure and Office applications:

The IT Services of ETH Zurich do not operate any mailboxes in the cloud. All mailboxes are operated in local data centres (on premises), not in the cloud.

With office applications, you have the option of storing and exchanging data in the cloud. However, you do not have to do this. Adhere to any specifications of the information owner.

This ensures that the above rules are adhered to.

More information:

Last update March 2022.

Please find further information on the regulation of external cloud services and classification of data and information at ETH Zurich here.

If you have any questions or would like further information, please contact:

ETH Zurich
IT Services - Service Desk
Tel: +41 44 632 77 77
E-Mail: servicedesk@id.ethz.ch