Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Regeln für die Nutzung externer Cloud-Dienste, die durch die Informatikdienste angeboten werden

Wenn Sie solche Cloud-Dienste nutzen (z.B. Microsoft 365, Zoom, Google Workspace), bestehen für Ihre Informationen besondere, d.h. cloud-spezifische Risiken.

Um Ihre Informationen zu schützen, gelten für Sie folgende Regeln:

1) Externe Cloud-Dienste dürfen auch mit vertraulichen Daten genutzt werden, wenn sie in der Freigabeliste für Nutzende erscheinen und der/die Informationseigner/in* damit einverstanden ist. Bei Zweifeln kontaktieren Sie den/die Informationseigner/in.
2) Wenn Sie **Zusatzdienste** wie Add-ins, Übersetzungsdienste, Literaturverwaltung, etc. verwenden, die nicht in der Freigabeliste aufgeführt sind, dann dürfen Sie darin keine vertraulichen, streng vertraulichen Daten oder Personendaten bearbeiten oder speichern.

* *Informationseignerinnen und -eigner sind verantwortlich für die Daten, die in ihrem Namen erhoben und bearbeitet werden. Diese entscheiden deshalb, wie stark ihre Daten zu schützen sind (durch die Klassifizierung der Vertraulichkeit) und ob diese in externe Cloud-Dienste ausgelagert werden dürfen. Informationseigner/innen können sein: Leitende von Organisationseinheiten (z.B. Abteilungs- und Stabsleitende, ProfessorInnen).*

Das bedeutet:

- Wenn Sie Informationen verwenden (hochladen, kommentieren, in einem Cloud Service teilen), die jemand anders erstellt hat, folgen Sie den Anweisungen dieser anderen Person. Bei Unklarheit fragen Sie die betreffende Person nach dem Klassifizierungsstatus.
- Fragen Sie in erster Linie den Informationseigner wie die Daten klassifiziert und verwendet werden müssen.
- Ist kein Informationseigner innerhalb der ETH bekannt, fragen Sie den Urheber/Autor.

Die cloud-spezifischen Risiken sind namentlich folgende:

- gewisse Abhängigkeit vom Cloud-Anbieter, z.B. bei Verfügbarkeit und Servicequalität
- möglicher Daten- oder Kontrollverlust beim Cloud-Anbieter
- möglicherweise komplizierte, uneinheitliche oder widersprüchliche Geschäftsbedingungen und Datenschutzbestimmungen beim Cloud-Anbieter
- womöglich ungünstige oder fehlende Haftungsregelungen im Schadenfall
- auch die Datenverschlüsselung bietet nur begrenzten Schutz
- bei Übernahme des Cloud-Anbieters oder Einstellung der Dienstleistung kann die Rückübertragung der Daten an die ETH zum Problem werden
- Cloud-Anbieter können durch ihre Regierung zur Offenlegung von Daten verpflichtet werden («lawful access»; insbesondere in den Vereinigten Staaten)
- Cloud-Dienste werden für Cyberattacken und (Industrie-)Spionage zunehmend attraktiver

Bei der Arbeit mit externen Cloud-Diensten ist es für die ETH Zürich wichtig, dass sie jederzeit Zugang zu und die Kontrolle über ihre Daten behält.

Beachten Sie auch, dass Sie der Bearbeitung von Daten in externen Cloud-Diensten keine Rechte Dritter, insbesondere Datenschutz- und Urheberrecht, verletzen.

Hinweis zur E-Mail-Infrastruktur und Office-Anwendungen:

Die Informatikdienste der ETH Zürich betreiben keine E-Mail-Postfächer in der Cloud. Alle E-Mail-Postfächer nur in lokalen Rechenzentren betrieben, nicht in der «Cloud».

Bei Office-Anwendungen haben Sie die Möglichkeit, Daten in der Cloud zu speichern und auszutauschen. Sie müssen dies aber nicht tun. Halten Sie sich an allfällige Vorgaben des Informationseigners.

Damit ist sichergestellt, dass die oben genannten Regeln eingehalten werden.

Weitere Informationen:

Letzte Aktualisierung März 2022.

Weitere Informationen zur Regelung von externen Cloud-Diensten und Klassifizierung von Daten und Informationen an der ETH Zürich finden Sie hier.

Falls Sie Fragen haben oder weitere Informationen wünschen, wenden Sie sich bitte an:

ETH Zürich
Informatikdienste - Service Desk
Tel: +41 44 632 77 77
E-Mail: servicedesk@id.ethz.ch