

# Leitlinien zur Nutzung von Cloud-Diensten

## an der Universität Duisburg-Essen

### vom 18. Juli 2019

---

#### Inhalt

Präambel .....	2
Beliebte Clouddienste und ihre Alternativen.....	3
Datenschutzrechtliche Aspekte.....	4
Dienstrechtliche Aspekte .....	4
Empfehlungen .....	5

Erarbeitet von der AG IT-Sicherheit unter Leitung des Informationssicherheitsbeauftragten (CISO)

Zustimmend zur Kenntnis genommen vom IKM-Vorstand auf seiner 98. Sitzung am 13. Juni 2019.

## **Präambel**

Die Nutzung von Cloud-Diensten zur Datenablage und –verarbeitung ist im privaten Umfeld allgegenwärtig. Gefördert wird dies auch durch die Verbreitung von Smartphones, die in der Regel nur mit einem Konto beim jeweiligen Anbieter nutzbar sind und Basisfunktionen wie Kontaktverwaltung und Terminplanung als Cloud-Dienst realisieren.

Auch für den dienstlichen Gebrauch ist die Nutzung zunehmend attraktiv: Die Nutzung ist meist sehr komfortabel und bereits aus dem privaten Umfeld bekannt. Der Zugriff von mehreren Endgeräten oder die Freigabe für andere Nutzer sind Funktionen, die auch für eine dienstliche Kooperation nützlich sein können.

Die dienstliche Cloud-Nutzung ist jedoch auch mit Risiken verbunden. So können die Nutzungsbedingungen dem Anbieter Rechte gewähren, die beim Umgang mit dienstlichen Daten unerwünscht sind oder die sogar dienstlichen Regelungen entgegenstehen.

Ziel dieses Dokuments ist es, Informationen für einen bewussten Umgang mit Cloud-Diensten zu liefern.

## Beliebte Clouddienste und ihre Alternativen

Dienst	Alternative	Bemerkungen
<b>Cloudspeicher</b> z.B. Dropbox, Onedrive, iCloud	<b>Sciebo</b> <a href="https://sciebo.de">https://sciebo.de</a>	Jeder Angehörige einer NRW-Uni kann seinen Account selbst aktivieren. 30 GB Speicherplatz persönlicher Account, 500 GB für Mitarbeiterinnen und bis 2 TB übertragbarer Projektspeicher für Gruppen ( <a href="https://www.uni-due.de/zim/services/sciebo/">https://www.uni-due.de/zim/services/sciebo/</a> )  Es ist empfehlenswert, Daten in der Cloud nur verschlüsselt abzulegen. Zur Erstellung verschlüsselter Container in Sciebo empfiehlt sich cryptomator ( <a href="https://cryptomator.org">https://cryptomator.org</a> )  Empfehlungen zur Ablage von Daten in Sciebo: „Datenkategorien und ihre Eignung zur sciebo-Cloud-Nutzung“
<b>Dateitransfer</b> z.B. Wetransfer	<b>Gigamove</b> <b>Sciebo</b>	Bei Sciebo per Link-Freigabe mit und ohne Passwort Die Verteilung personenbezogener Daten per offenem Link ist zu vermeiden.
<b>Messenger/Chat</b> z.B. WhatsApp, Telegram, Threema, Signal, Slack	<b>Jabber-Server der Uni</b> <a href="https://www.uni-due.de/zim/services/weitere_internetdienste/jabber.shtml">https://www.uni-due.de/zim/services/weitere_internetdienste/jabber.shtml</a>	Jabber kann auf Smartphones z.B. mit Xabber als Client genutzt werden. Threema lässt sich datenschutz-konform nutzen Whatsapp ist zur beruflichen Nutzung nicht zulässig, da bei der Installation personenbezogene Daten anderer Nutzer ohne deren Wissen weitergegeben werden (alle Kontakte auf dem Smartphone)
<b>Online-Kalender</b> z.B. Google-Kalender	<b>Exchange der UDE</b> <b>BSCW</b>	Eine wünschenswerte Ergänzung wäre die Aktivierung der Kalender-Funktion in Sciebo oder eine eigene CalDAV-Lösung per Nextcloud/Owncloud
<b>Online-Terminfindung</b> z.B. Doodle	<b>Foodle</b> <a href="https://terminplaner.dfn.de/">https://terminplaner.dfn.de/</a> <b>BSCW</b>	
<b>Videokonferenzen</b> Skype, BlueJeans, Zoom	<b>Pexip</b> <b>Adobe Connect über</b> <b>DFN-Verein</b> <a href="https://conf.dfn.de">https://conf.dfn.de</a>	Bei der freien Skype-Variante hat Microsoft per Nutzungsvereinbarung Rechte an Inhalten der Konferenz
<b>Online-Kollaboration (Online-Büroprogramme)</b> z.B. Google Docs, Office 365 TeX: Overleaf, Sharelatex	<b>Sciebo (Onlyoffice)</b> <a href="https://sciebo.de/analyse/editor.html">https://sciebo.de/analyse/editor.html</a>	Eine wünschenswerte Ergänzung wäre die Bereitstellung von Sharelatex auf einem eigenen Server der UDE ( <a href="https://github.com/sharelatex/sharelatex">https://github.com/sharelatex/sharelatex</a> )

<b>Versionsverwaltung</b> z.B. Github, Gitlab, Bitbucket	<b>Gitlab-Server der Uni</b> <a href="https://git.uni-due.de">https://git.uni-due.de</a>	
<b>Soziale Medien</b> z.B. Facebook, Instagram, Twitter, YouTube	Diaspora <b>eigene Blogs</b> <a href="https://blogs.uni-due.de">https://blogs.uni-due.de</a>	
<b>Befragungs- und Feedbackwerkzeuge</b> z.B. Unipark, SocSciesurvey etc.	<b>Limesurvey an der UDE</b> <b>Pingo an der UDE</b> <a href="https://pingo.uni-due.de">https://pingo.uni-due.de</a>	

## Datenschutzrechtliche Aspekte

Im Kern der datenschutzrechtlichen Betrachtung liegt in der Regel eine Offenlegung von Daten gegenüber Dritten was die Vertraulichkeit gefährdet. Die Einsichtnahme von Dritten muss in einer Weise eingeschränkt sein, die dem Schutzbedarf der Daten entspricht. Dabei können sind Einsichtnahmemöglichkeiten von weiteren Personen, die einen Dienst nutzen können, die des Dienstbetreibers und auch weitere beispielsweise staatliche Institutionen zu bedenken.

In der Regel werden die Dienste als Datenverarbeitung im Auftrag genutzt. In einem solchen Fall ist eine entsprechende rechtliche Vereinbarung erforderlich (AV Vertrag nach Art. 28 DSGVO). Solche Verträge liegen beispielsweise bei dem Dienst Sciebo vor. Sollte ein Dienst durch einen außereuropäischen Anbieter betrieben werden, so sind weitere Anforderungen zu erfüllen (Art. 44 ff. DSGVO). Bei einer einfachen Nutzung mit einem Nutzungsvertrag werden die Anforderungen zumeist nicht erfüllt.

Auch bei einer grundsätzlich zulässigen Nutzung eines Dienstes, muss entsprechend der Schadenszenarien/des Schutzbedarfs der Daten ein angemessener Schutz gewährleistet sein. So ist beispielsweise für den Dienst Sciebo eine Empfehlung verfügbar, in der bestimmt wird, in welchen Fällen eine Nutzung zulässig ist.

Die Schutzziele Verfügbarkeit (und meist auch Integrität) sind bei großen Anbietern in der Regel gut gewährleistet. Eigene Dienste bieten aber vergleichbares Niveau. Ein Backup wichtiger Daten ist ohnehin sinnvoll, vor allem bei gemeinsamer Arbeit an einem Datenbestand.

## Dienstrechtlche Aspekte

Die dienstliche Nutzung von Cloud-Diensten erfolgt nicht isoliert, sondern ist Teil eines IT-Verfahrens. Daher müssen insbesondere bei Einführung oder Änderung die Regelungen der „Rahmen-Dienstvereinbarung IT“ berücksichtigt werden.

Rahmen-Dienstvereinbarung IT: [https://www.uni-due.de/imperia/md/content/zentralverwaltung/formulare/rahmen\\_dienstvereinbarung\\_it.pdf](https://www.uni-due.de/imperia/md/content/zentralverwaltung/formulare/rahmen_dienstvereinbarung_it.pdf)

IT-Verfahren, die gemäß den Regelungen der „Rahmen-Dienstvereinbarung IT“ eingeführt oder geändert wurden, können grundsätzlich als dienstrechtlich unbedenklich betrachtet werden.

## Empfehlungen

Es ist grundsätzlich empfehlenswert, universitätsnahe Dienste den öffentlichen Angeboten vorzuziehen. Öffentliche Angebote sind auf den ersten Blick kostenlos, das Geschäftsmodell der Anbieter basiert allerdings meist auf der Auswertung der Daten des Nutzers. Dies ist bei Diensten von zum Beispiel der Universität oder des DFN-Vereins nicht der Fall. Die rechtlichen Rahmenbedingungen im Einzelfall sind dabei zu beachten.

**Prüfen Sie vor der Nutzung eines öffentlichen Cloud-Dienstes, ob die Anforderungen nicht auch von hauseigenen Diensten erfüllt werden können.**

Für viele beliebte Anwendungen werden im universitären Umfeld hauseigene Dienste angeboten. Einige Nutzungsempfehlungen finden Sie im Abschnitt „Beliebte Cloud-Dienste und ihre Alternativen“. Für Dienste ohne hauseigene Alternative kann es abhängig vom Bedarf vorteilhaft sein, ein entsprechendes zentrales Angebot an der UDE einzuführen. Hierzu empfiehlt sich eine entsprechende Kooperation der Institute und zentralen Einrichtungen.

Vor der Nutzung von Cloud-Diensten ist es ratsam, den Schutzbedarf der verarbeiteten Daten hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität zu analysieren. Eine Orientierung über gängige Datenkategorien und ihre Schutzbedarfe liefert die Aufstellung zur Speicherung von Daten in Sciebo. Bei der Verwendung anderer Dienste sollen diese Empfehlungen entsprechend nicht unterschritten werden.

Sciebo-Verschlüsselung: <https://www.uni-due.de/zim/services/sciebo/verschluesselung.php>

Datenkategorien: [https://www.uni-due.de/imperia/md/content/zim/aktuelles/datenkategorien\\_und\\_ihre\\_eignung\\_zur\\_cloud.pdf](https://www.uni-due.de/imperia/md/content/zim/aktuelles/datenkategorien_und_ihre_eignung_zur_cloud.pdf)

Bei grundsätzlichen Überlegungen zur Nutzung von Cloud-Diensten, die über die hier empfohlenen Dienste hinausgehen, bieten sich die Mindeststandards des BSI zur Nutzung von Cloud-Diensten als weitergehende Informationsquelle an.

Mindeststandards für Cloud-Dienste:

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard\\_Nutzung\\_externer\\_Cloud-Dienste.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste.pdf)

Sichere Nutzung von Cloud-Diensten:

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere\\_Nutzung\\_Cloud\\_Dienste.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf)

Goldene Regeln zur Cloud-Nutzung:

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/IT-GS-Bausteine/Cloud\\_Nutzung/Goldene-Regeln-Cloud-Nutzung.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/IT-GS-Bausteine/Cloud_Nutzung/Goldene-Regeln-Cloud-Nutzung.pdf)

Ausgefertigt aufgrund des Beschlusses des Rektorats vom 17. Juli 2019

Duisburg und Essen, den 18. Juli 2019

Für den Rektor der Universität Duisburg-Essen  
Der Kanzler In Vertretung  
Sabine Wasmer