

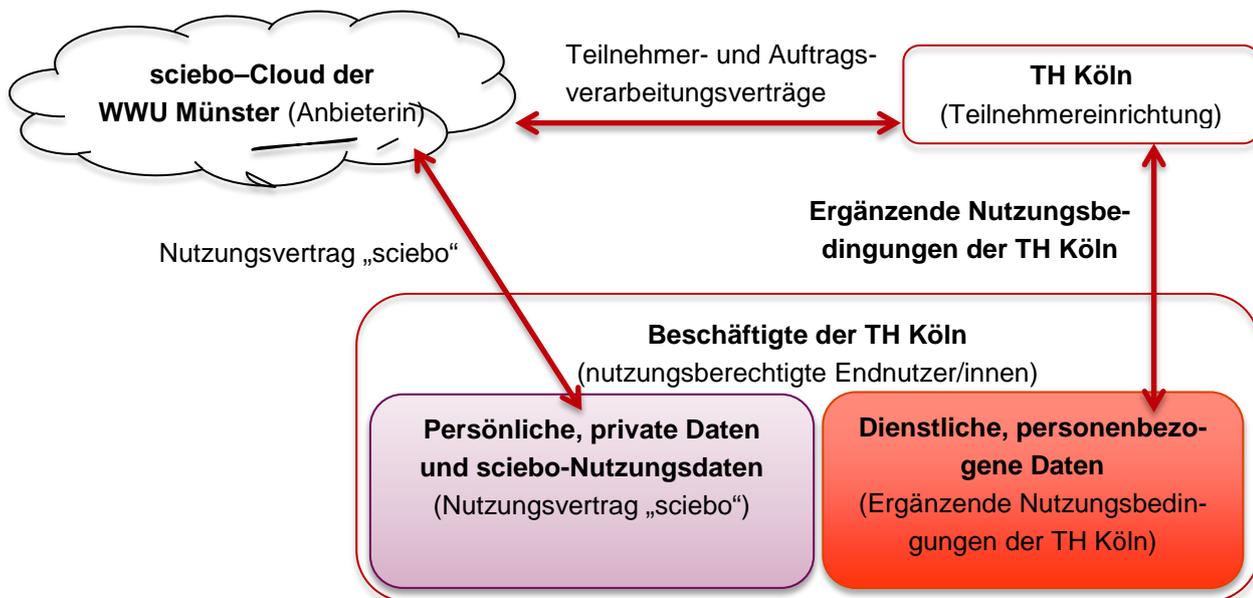
## Ablage von dienstlichen Daten in dem Cloud-Speicherdienst „sciebo“ (www.sciebo.de)

Stand 21.05.2019

Dieses Merkblatt richtet sich an Beschäftigte der TH Köln, die den Cloud-Speicherdienst „sciebo“ im Zusammenhang mit dienstlichen, personenbezogenen Daten nutzen möchten.

### 1.1 Neugestaltung der Vertragsbeziehungen

Wegen privater sowie dienstlicher Nutzungsmöglichkeiten von sciebo mussten die Rechtsbeziehungen angepasst werden, so dass sich nun die Endnutzer/innen der TH Köln persönlich bei sciebo registrieren und einen (End-) Nutzungsvertrag „sciebo“ mit der WWU Münster als alleinige Anbieterin abschließen müssen. Die Ablage bzw. Verarbeitung dienstlicher Daten der Beschäftigten der TH Köln in der sciebo-Cloud unterliegen den ergänzenden Nutzungsbedingungen der TH Köln, die bitte von allen Beschäftigten bei Nutzung der sciebo-Cloud mit dienstlichen Daten zu beachten sind.



### 1.2 Was sind dienstliche, personenbezogene Daten?

Unter „dienstlichen, personenbezogenen Daten“ sind alle personenbezogenen Daten von natürlichen Personen zu verstehen, die im Rahmen der dienstlichen Tätigkeit rechtmäßig von Dritten erhoben worden sind und in die sciebo-Cloud zur weiteren Verarbeitung (z.B. speichern, synchronisieren, teilen, übermitteln, verändern oder zum Abruf bereitstellen) eingebracht werden. Darunter fallen nicht Ihre eigenen personenbezogenen Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes von der Anbieterin erhoben und verarbeitet werden. Die von Ihnen eingebrachten dienstlichen Daten werden nur im Auftrag und auf Ihre Weisung (z.B. Übermittlung aufgrund Ihrer Dateifreigabe) durch die Anbieterin verarbeitet.

### 1.3 Kompakt: Was muss ich vor der Ablage von dienstlichen Daten besonders beachten?

- Die sciebo-Cloud sollte grundsätzlich nur zum Synchronisieren von Daten über eigene Endgeräte oder zum gemeinsamen Bearbeiten und Teilen von Dokumenten genutzt werden.
- Die **Nutzung der sciebo-Cloud mit besonders schützenswerten, dienstlichen Daten (wie personenbezogene Daten Dritter oder sensible geheimhaltungsbedürftiger Daten)** unterliegt besonderen Sicherheitsanforderungen und erfordert einen sorgsamen Umgang und die Beachtung der gesetzlichen Vorschriften, wie EU-DS-GVO und DSGVO NRW sowie der Bestimmungen des Nutzungsvertrags und der ergänzenden Nutzungsbedingungen der TH Köln.
- Nehmen Sie bitte eine **strikte Trennung von persönlichen, privaten Daten und dienstlichen Daten** vor, z.B. durch unterschiedliche Dateierdner wie „Privat“ und „Dienstlich“.
- Bei **Einsatz von Dateiverschlüsselung** ist ein sicheres Verfahren und ein Schlüssel- bzw. Passwortmanagement unabdingbar. Ein Verlust des Schlüssels bzw. Passworts führt i.d.R. zu einem Totalverlust der Daten, sofern Sie zuvor keine Backups der (unverschlüsselten) Daten angefertigt haben.
- Der Dienst ist nicht als Backuplösung geeignet. Die Anbieterin stellt lediglich die jederzeitige Datenverfügbarkeit sicher und führt **keine Datensicherungskopien (Backups)** durch. Sollten Sie als Nutzer/in oder ggf. andere Nutzer/innen oder eingeladene Gäste, denen Sie Datei- oder Ordnerfreigaben erteilt haben, versehentlich Ihre Dateien löschen, so sind die Daten i.d.R. unwiederbringlich verloren. Sie sind daher selbst für eine ordnungsgemäße Datensicherung (Backups) Ihrer in sciebo verarbeiteten Daten verantwortlich.
- Prüfen Sie, ob die sciebo-Cloud für die Ablage Ihrer dienstlichen Daten geeignet ist. Hierzu ist vor dem Hochladen der Daten zunächst der Schutzbedarf gemäß den Nutzungsbedingungen der TH Köln festzustellen. Weitere Informationen und Beispiele finden Sie in den „Ergänzenden Nutzungsbedingungen des Cloud-Storage-Dienstes sciebo für die Auslagerung von dienstlichen Daten“ der TH Köln.
- **Daten mit sehr hohem Schutzbedarf dürfen nicht in sciebo gespeichert werden**, z.B. Personalaktendaten, wissenschaftliche Daten mit sehr hohem Schutzbedarf (abhängig von Inhalt, wie Untersuchungsergebnisse, vertrauliche Forschungsdaten etc.), dienstliche (nicht wissenschaftliche) Daten (z.B. Gesundheitsdaten, ärztliche Diagnosen etc.) und ggf. Daten, die besonderen Geheimhaltungsvereinbarungen unterliegen.
- Weiterhin **dürfen besonders sensible personenbezogene Daten i.S.d. Art. 9 DS-GVO nicht in dem Dienst gespeichert werden** (z.B. über ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur Personenidentifizierung, Gesundheitsdaten, Sexualleben und sexuelle Orientierung)
- **Dienstliche, personenbezogene Daten mit hohem Schutzbedarf** erfordern stärkere Schutzmaßnahmen und sollten grundsätzlich nur verschlüsselt in dem Dienst gespeichert werden (z.B. Prüfungsergebnisse, Notenlisten, Gutachten, ggf. auch wissenschaftliche Daten, Video- und Audioaufnahmen von Befragungen (abhängig von Inhalt)

### 1.4 Wo kann ich weitere Informationen und Hilfen zu sciebo finden?

Weitere Bestimmungen, Informationen und Beispiele finden Sie in Ihrem Nutzungsvertrag „sciebo“ (<https://www.sciebo.de/agb/>) und in den **ergänzenden Nutzungsbedingungen des Cloud-Storage-Dienstes „sciebo“ für die Auslagerung von dienstlichen Daten der TH Köln** (abrufbar unter <https://www.th-koeln.de/sciebo/>).

Weitere Informationen, Antworten auf häufig gestellte Fragen und Hilfe zu „sciebo“ finden Sie unter:

- Helpcenter der Anbieterin (<https://sciebo.de/de/hilfe/>)
- Service-Webseite “sciebo” der Campus IT (<https://www.th-koeln.de/sciebo/>)
- Servicedesk der Campus IT ([support@campus-it.th-koeln.de](mailto:support@campus-it.th-koeln.de)).

Bei datenschutzrechtlichen Fragen, z.B. zum Schutzbedarf personenbezogener Daten, wenden Sie sich bitte ggf. über Ihre/n Datenschutzkoordinator/in an den Datenschutzmanager der TH Köln ([datenschutzmanager@th-koeln.de](mailto:datenschutzmanager@th-koeln.de)).