Technology
Arts Sciences
TH Köln

Campus IT
Tel. +49 221 / 8275 - 2323
Fax +49 221 / 8275 - 2660
Technische Hochschule Köln
Betzdorfer Strasse 2
D 50679 Köln
support@campus-it.th-koeln.de
http://www.th-koeln.de

Ergänzende Nutzungsbedingungen des Cloud-Storage-Dienstes „sciebo“ für die Auslagerung von dienstlichen Daten

vom 13.05.2019

Inhalt

Aufgrund des § 2 Absatz 2 der Benutzungsordnung für die zentralen IT-Services der Campus IT hat die Campus IT der Technischen Hochschule Köln (im Folgenden „TH Köln“) die folgenden ergänzenden Nutzungsbedingungen zur Auslagerung von dienstlichen Daten in den Cloud-Storage-Dienst „sciebo“ (im Folgenden „sciebo-Dienst“) erlassen:

Präambel

Diese Nutzungsbedingungen ergänzen und konkretisieren die grundsätzlichen Regelungen des Nutzungsvertrages zwischen der Westfälischen Wilhelms-Universität Münster (im Folgenden „Anbieterin“) und dem/der Endnutzer*in (abrufbar unter www.sciebo.de/agb/) über die Bereitstellung des Cloud-Storage-Dienstes „sciebo“ zu Zwecken von Forschung, Lehre und Hochschulverwaltung in Bezug auf die **dienstliche Nutzung des Cloud-Storage-Dienstes „sciebo“ für die Datenablage von personenbezogenen Daten im Rahmen der dienstlichen Tätigkeit** durch Mitglieder der Technischen Hochschule Köln.

Wenn Daten mit Hilfe von weltweit jederzeit verfügbaren Cloud-Speicherdiensten an dynamisch verteilten Orten gespeichert bzw. verarbeitet werden, drohen besondere Gefahren. Diesen Risiken ist mit einer spezifischen Vorsorge hinsichtlich der Informationssicherheit und des Schutzes personenbezogener Daten zu begegnen.

Für die Speicherung und Verarbeitung gilt insbesondere die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, nachfolgend „DSGVO“), das Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) und ggf. weitere nationale datenschutzrechtliche Regelungen (insbesondere das BDSG).

Die Nutzer*innen der TH Köln sind für die bestimmungsgemäße Nutzung der sciebo-Cloud und der Einhaltung der Regelungen sowie für die sorgfältige Trennung zwischen privaten und dienstlichen Daten selbst verantwortlich.

Für **private Daten** der Endnutzer*innen gilt alleine der (End-)Nutzungsvertrag zwischen der Anbieterin und dem/der Endnutzer*in. Die Anbieterin ist diesbezüglich alleinige Verantwortliche im Sinne des Art. 4 S. 1 Nr. 7 DSGVO.

Für **dienstliche, personenbezogene Daten** der Nutzer*innen der TH Köln, die im Rahmen ihrer dienstlichen Tätigkeit durch die Anbieterin verarbeitet werden sollen, gelten diese ergänzenden Nutzungsbedingungen. In Bezug auf die dienstlichen, personenbezogenen Daten gilt die TH Köln als Verantwortliche im Sinne des Art. 4 S.1 Nr. 7 DSGVO. Die Verarbeitung von dienstlichen, personenbezogenen Daten erfolgt durch die Anbieterin nur auf Weisung und im Auftrag der TH Köln.

§ 1 Geltungsbereich

(1) Diese Nutzungsbedingungen beinhalten ergänzend zu den Bestimmungen aus dem „sciebo“-Nutzungsvertrag zwischen Endnutzer*in und der Anbieterin grundsätzliche Nutzungsregelungen für alle Nutzer*innen der Technischen Hochschule Köln, wenn Sie in Ausübung der dienstlichen Tätigkeit für die Technische Hochschule Köln den Cloud-Storage-Dienst „sciebo“ zur Datenablage von dienstlichen, personenbezogenen Daten nutzen möchten, die durch die Anbieterin im Auftrag der TH Köln erhoben, gespeichert und verarbeiten werden.

(2) Diese Nutzungsbedingungen finden auf private Daten der Endnutzer*in im Sinne des § 2 Abs. 5 keine Anwendung.

§ 2 Abgrenzung und Begriffsdefinitionen

(1) „Personenbezogene Daten“ sind alle Informationen im Sinne des Art. 4 Nr. 1 DS-GVO, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine natürliche Person wird als identifizierbar angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

(2) „Besondere Kategorien personenbezogener Daten“ im Sinne des Art. 9 Abs. 1 DSGVO sind besonders sensible personenbezogene Daten. Hierunter fallen:

- Daten, aus denen die rassische und ethnische Herkunft hervorgeht,
- Daten, aus denen politische Meinungen hervorgehen,
- Daten, aus denen religiöse oder weltanschauliche Überzeugungen hervorgehen,
- Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht,
- genetische Daten im Sinne des Art. 4 Nr. 13 DSGVO,
- biometrische Daten im Sinne des Art. 4 Nr. 14 DSGVO), die zur eindeutigen Identifizierung einer natürlichen Person verarbeitet werden,
- Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) und
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(3) „Sachbezogene Daten“ sind Daten ohne Personenbezug im Sinne des Absatzes 1. Diese Daten können auch einen hohen Schutzbedarf haben, insbesondere wenn Sie ein Dienst- oder Geschäftsgeheimnis darstellen oder einer Vertraulichkeits- oder Geheimhaltungsvereinbarung unterliegen.

(4) „Dienstliche personenbezogene Daten“ sind personenbezogene Daten im Sinne des Absatzes 1, die durch den/die Endnutzer*in in Ausübung einer dienstlichen Tätigkeit zu Zwecken der Lehre, Forschung und Hochschulverwaltung in die sciebo-Cloud eingebracht und verarbeitet werden.

(5) „Private Daten der Endnutzer*in“ sind personenbezogene Daten, die durch den/die Endnutzer*in als natürliche Personen zur Ausübung ausschließlich privater bzw. persönlicher Tätigkeiten in die sciebo-Cloud eingebracht und verarbeitet werden.

§ 3 Schutzbedarf

(1) Für die Entscheidung, unter welchen Bedingungen eine Auslagerung von dienstlichen, personenbezogenen Daten in die sciebo-Cloud in Frage kommt, bildet der Schutzbedarf der dienstlichen, personenbezogenen Daten die grundlegende Richtschnur. Hinweise auf den Schutzbedarf können zum einen aus der systematisch durchgeführten Schutzbedarfsanalyse und zum anderen aus der Datenkategorie abgeleitet werden.

(2) Daten lassen sich in die folgenden **Datenkategorien** einteilen:

Datenkategorie	**Hinweis auf typischen Schutzbedarf**
Daten, die aus öffentlich zugänglichen und offenkundig legal zugänglichen Quellen stammen (z.B. Literatur und Dokumente)	Keinen
Sachbezogene Daten, die keine personenbezogenen Daten beinhalten	Keinen bis sehr hoch
Dienstliche (nicht wissenschaftliche) Daten	Normal bis sehr hoch
Dienstliche (nicht wissenschaftliche) Daten, z.B. Lehrveranstaltungsdaten (Teilnehmendenlisten)	Normal
Dienstliche (nicht wissenschaftliche) Daten, z.B. Fotos und Videos von öffentlichen Veranstaltungen ohne, dass hierdurch Einzelpersonen oder kleine Gruppen hervorgehoben werden	Normal
Dienstliche (nicht wissenschaftliche) Daten, z.B. Prüfungsdaten (Prüfungsergebnisse, Notenlisten, Gutachten)	Hoch
Handgeschriebene Texte mit personenbezogenen Daten (z.B. Vor- und Nachname, Matrikelnummer etc.)	Hoch
Dienstliche (nicht wissenschaftliche) Daten, z.B. Video- und Audioaufnahmen von Befragungen (abhängig von Inhalt)	Hoch bis sehr hoch
Wissenschaftliche Daten	Normal bis sehr hoch
Wissenschaftliche Daten, z.B. Untersuchungsergebnisse, vertrauliche Forschungsdaten	Hoch bis sehr hoch
Besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO: Gesundheitsdaten, politische Meinungen, Daten über die sexuelle Orientierung, biometrische Identifikations- und Verifikationsdaten (wie DNA, Augenablichtung, Gesichtsgeometrie, Fingerabdrücke, Stimme) etc.	Sehr hoch
Personalaktendaten	Sehr hoch

In jedem Fall sind die folgenden Aspekte zu beachten:

- Für personenbezogene Daten gelten die Bestimmungen des Datenschutzes
- Auch Daten ohne Personenbezug (sachbezogene Daten) können einen sehr hohen Schutzbedarf haben (zum Beispiel auf Grund von Vertraulichkeits- oder Geheimhaltungsvereinbarungen).

(3) Der **Schutzbedarf** wird grundsätzlich hinsichtlich der drei Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit differenziert bestimmt. Entsprechend differenziert sollten Vorkehrungen zur Sicherheit der Daten getroffen werden. Aus dem Schutzbedarf der Daten folgt zwingend die Eignung oder Nicht-Eignung zur Speicherung in sciebo-Cloud:

Schutzbedarf	Eignung für die Ablage
Daten mit keinem oder normalen Schutzbedarf	Ja
Daten mit hohem Schutzbedarf	Nur verschlüsselt
Daten mit sehr hohem Schutzbedarf	Nein

Empfehlungen

Bevor Daten in der sciebo-Cloud abgelegt werden, sollten die im vorangegangenen Abschnitt betrachteten Abhängigkeiten zwischen der Datenkategorie, dem Schutzbedarf der Daten und der Eignung beachtet werden.

Sparsamer Umgang

Prinzipiell sollte bei der Nutzung der sciebo-Cloud die Datenmenge auf das notwendige Mindestmaß begrenzt werden. Beispielsweise kann bei der Übertragung ganzer Verzeichnisbäume in die Cloud leicht übersehen werden, dass in einem Unterverzeichnis sensible Daten abgelegt wurden, die den Bereich der Einrichtung nicht verlassen dürfen. Bevor Daten auf Endgeräten synchronisiert werden, sollten erwarteter Nutzen und damit verbundene Risiken gegeneinander abgewogen werden.

Schutzbedarf der Daten bestimmt den Umfang der Cloud-Nutzung

Aus dem Schutzbedarf der für eine Speicherung vorgesehenen Daten folgt nicht nur, ob eine Speicherung zulässig ist, sondern auch unter welchen Bedingungen dies geschehen kann. Dabei ist der Schutzbedarf getrennt nach den drei Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit zu betrachten.

Verfügbarkeit

Die Daten in der sciebo-Cloud befinden sich an einem von drei Hochschulstandorten in NRW. Es gibt keine serverseitigen Backups der Daten. Beim Ausfall eines Standorts könnten die Daten daher zeitweise oder dauerhaft nicht für den Zugriff oder zur Synchronisation zur Verfügung stehen. Die TH Köln haftet nicht für Schäden aus dem Verlust von Daten. Endnutzer*innen sind für Datensicherungen verantwortlich.

Wenn sehr hohe Anforderungen an die Verfügbarkeit gestellt werden, kommt eine Datenablage in der sciebo-Cloud nicht in Frage.

Integrität

Die technische Sicherstellung der Datenintegrität erfolgt durch spezielle Speichersysteme. Die Wahrscheinlichkeit von unerkannten Fehlern in den Daten ist sehr gering, aber nicht

ausgeschlossen. Auf Grund der Nutzung über das Internet und der höheren Nutzerzahl bietet die sciebo-Cloud eine größere Angriffsfläche als Dienste, die ausschließlich hochschulintern angeboten werden. Im Falle von Sicherheitslücken in der verwendeten Systemsoftware oder kompromittierten Zugangsdaten ist eine Datenmanipulation durch unberechtigte Personen möglich.

Wenn in dieser Hinsicht hohe oder sogar sehr hohe Anforderungen bestehen, sollte die/der Nutzer*in selbst geeignete Maßnahmen zur Gewährleistung der Integrität ergreifen. Beispielsweise können Prüfsummen verwendet werden, mit deren Hilfe eine Veränderung an den Daten erkannt werden kann. In Systemen zur Datenverschlüsselung sind derartige Verfahren in der Regel bereits integriert.

Vertraulichkeit

Die Nutzerdaten werden durch die Anbieterin nicht an Dritte, insbesondere nicht an Privatunternehmen, weitergegeben, nicht durch diese verarbeitet und auch nicht außerhalb des Gebietes der Bundesrepublik Deutschland abgespeichert. Die Sciebo-Cloud bietet jedoch eine größere Angriffsfläche als ein nur hochschulintern angebotener Dienst (z.B. nur intern erreichbare Netzlaufwerke der Campus IT). Im Falle von Sicherheitslücken in der verwendeten Systemsoftware oder kompromittierten Zugangsdaten könnten unberechtigte Personen an vertrauliche Daten gelangen.

Wenn hohe Anforderungen an die Vertraulichkeit gestellt werden, ist als adäquate Maßnahme der Einsatz eines Datenverschlüsselungssystems (Dateiverschlüsselung, verschlüsselte Dateicontainer etc.) zwingend notwendig. Es wird keine serverseitige Verschlüsselung angeboten, da diese keinen ausreichenden Schutz bietet. Darum sollte der Verschlüsselungsprozess lokal vorgenommen werden, bevor die Daten in die Cloud übertragen werden. Die Sicherheit verschlüsselter Daten hängt u.a. von der Qualität des Verschlüsselungsalgorithmus, der Verschlüsselungssoftware, der Schlüssellänge und dem Schlüsselmanagement ab. Beim Einsatz von Verschlüsselung sollte darauf geachtet werden, dass die von der Campus IT als Standard vorgegebene Anwendung genutzt wird. Außerdem muss zwingend darauf geachtet werden, dass die Verschlüsselung der Daten vor der Dateiübertragung an die sciebo-Cloud bzw. außerhalb des Synchronisationsordners auf den Endgeräten erfolgt, so dass keine unverschlüsselten Daten (auch keine temporären Dateien) mit der sciebo-Cloud synchronisiert werden. Gleiches gilt für die Entschlüsselung der Daten, die nicht innerhalb der sciebo-Cloud oder innerhalb des lokalen Synchronisationsordners auf den Endgeräten erfolgen darf.

(4) **Bei Daten mit sehr hohen Anforderungen an die Vertraulichkeit (insbesondere bei besonders sensiblen personenbezogenen Daten im Sinne des Art. 9 Abs. 1 DSGVO (vgl. § 2 Abs. 2) ist grundsätzlich von der Ablage in der sciebo-Cloud abzusehen.**

§ 4 Schutzbedarfsanalyse

(1) Mit dem folgenden Fragenkatalog soll der Schutzbedarf der zu verarbeitenden Daten festgestellt werden. Der Fragenkatalog ist angelehnt an die Richtlinien zum IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Der Schutzbedarf definiert sich dabei ausschließlich aus den anzunehmenden Schäden, die entstehen, wenn die Daten nach einem auslösenden Ereignis (durch spezifische Bedrohungen wie Passwortkompromittierung, Ausfall eines Dienstes, Verlust eines Datenträgers etc.) beeinträchtigt werden und so mindestens einer der Grundwerte der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit) verletzt wird. Dabei ergibt sich der Schutzbedarf aus den unmittelbaren Schäden und durch die möglichen Folgeschäden (z.B. Schadensersatzforderungen, Produktionsausfallkosten).

Eine quantitative Bewertung mit bezifferten Schadenshöhen wäre hier zu aufwendig und ist unter verschiedenen Aspekten auch kaum möglich (z.B. negative Außenwirkungen, "Ruf der Institution", Schädigung durch Ansehensverlust). Vielmehr soll die persönliche Wertung helfen, eine relative Bewertung aufzustellen, die für die Notwendigkeit und Umsetzung von Schutzmaßnahmen eine Dringlichkeitsreihenfolge ergibt.

Insgesamt handelt es sich um vier Themenbereiche, die aus sicherheitsrelevanten Gesichtspunkten beleuchtet werden. Diese sind:

- Verstöße gegen Gesetze,
- Beeinträchtigungen der Unversehrtheit,
- Beeinträchtigungen der Aufgabenerfüllung und
- Finanzielle Auswirkungen.

Diese Themenbereiche werden betrachtet unter den Aspekten:

- Integrität/Vertraulichkeit der Daten und
- Verfügbarkeit der Daten und Dienste.

§ 5 Schutzbedarfskategorien

(1) Schutzbedarfskategorie „Keine“:

Schäden haben nur eine unwesentliche Beeinträchtigung der Person oder der Institution oder einer anderen an der sciebo-Cloud teilnehmenden Institutionen zur Folge.

Vertraulichkeit und Integrität der Daten	
Verstoß gegen Gesetze und Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze ohne nennenswerte Konsequenzen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts ist nicht nennenswert. Ein möglicher Missbrauch personenbezogener Daten hat keine nennenswerten Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der/des Betroffenen.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung ist nicht nennenswert.
Negative Außenwirkung	Es ist keine nennenswerte Ansehens- oder Vertrauensbeeinträchtigung zu erwarten.
Finanzielle Auswirkungen	Es ist kein nennenswerter finanzieller Schaden zu erwarten.
Verfügbarkeit der Daten	

Beeinträchtigung der Aufgabenerfüllung	Es ist keine oder nur eine äußerst geringe Beeinträchtigung zu erwarten. In Ausnahmefällen liegt die maximal tolerierbare Ausfallzeit bei bis zu zwei Tagen.

(2) Schutzbedarfskategorie „Normal“:

Schäden haben Beeinträchtigungen der Institution oder anderer an der sciebo-Cloud teilnehmenden Institutionen zur Folge.

Vertraulichkeit und Integrität der Daten	
Verstoß gegen Gesetze und Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als tolerabel eingeschätzt werden. Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der/des Betroffenen.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung erscheint nicht möglich.
Negative Außenwirkung	Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der finanzielle Schaden bleibt für die Institution tolerabel.
Verfügbarkeit der Daten	
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen bei bis zu 8 Stunden.

(3) Schutzbedarfskategorie „Hoch“:

Im Schadenfall tritt Handlungsunfähigkeit wichtiger Bereiche der Institution oder anderer an der sciebo-Cloud teilnehmenden Institutionen ein; Schäden haben erhebliche Beeinträchtigungen der Institution selbst, anderer an der sciebo-Cloud teilnehmenden Institutionen, oder betroffener Dritter zur Folge.

Vertraulichkeit und Integrität der Daten	
Verstoß gegen Gesetze und Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen Vertragsverletzungen mit hohen Konventionalstrafen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
Negative Außenwirkung	Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der Schaden bewirkt beachtliche finanzielle Verluste, ist je-

	doch nicht existenzbedrohend.
Verfügbarkeit der Daten	
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von einzelnen betroffenen Personen als nicht tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen bei bis zu 4 Stunden.

(4) Schutzbedarfskategorie „Sehr hoch“:

Der Schadenfall führt zum totalen Zusammenbruch der Institution oder anderer an der sciebo-Cloud teilnehmenden Institutionen, oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche, oder es besteht Gefahr für Leib und Leben von Personen.

Vertraulichkeit und Integrität der Daten	
Verstoß gegen Gesetze und Vorschriften/Verträge	Fundamentaler Verstoß gegen Vorschriften und Gesetze Vertragsverletzungen, deren Haftungsschäden ruinös sind.
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
Beeinträchtigung der persönlichen Unversehrtheit	Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. Gefahr für Leib und Leben.
Negative Außenwirkung	Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenzgefährdender Art, ist denkbar.
Finanzielle Auswirkungen	Der finanzielle Schaden ist für die Institution existenzbedrohend.
Verfügbarkeit der Daten	
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen unter einer Stunde.

Weitere Informationen

[1] Arbeitskreis der Leiter Wissenschaftlicher Rechenzentren in NRW (ARNW), „Regelungen zur IT-Sicherheit in der Universität Münster,“ 21 Feb 2002. [Online]. Abrufbar unter: http://www.uni-muenster.de/Rektorat/abuni/ab020507.html.
[2] T. Rensing, „ISidoR Onlinedokumentation,“ 24 November 2010. [Online]. Abrufbar unter: http://www.nic.uni-muenster.de/Sec_Glossar/sec_handbuch.asp.

§ 6 Nutzungsberechtigung und Registrierung

(1) Nutzungsberechtigt sind alle Mitglieder und Angehörigen der Technischen Hochschule Köln.

(2) Die Campus IT der TH Köln stellt Ihnen, wenn Sie nutzungsberechtigt sind, einen Identity Provider (IdP) zur Verfügung.

Dieser dient der Authentifizierung und Autorisierung der Mitglieder und Angehörigen der TH Köln gegenüber externen Dienstanbietern, sogenannten Service Providern (SPs), im Rahmen der Infrastruktur für Authentifizierung und Autorisierung des Vereins zur Förderung eines Deutschen Forschungsnetzes e.V. (DFN-AAI). Die Authentifizierungs- und Autorisierungs-Infrastruktur DFN-AAI wird vom DFN-Verein verwaltet. Er schafft das notwendige Vertrauensverhältnis sowie einen organisatorischen und technischen Rahmen für den Austausch von Benutzerinformationen zwischen den teilnehmenden Einrichtungen, zu denen auch die TH Köln gehört, und Drittanbietern (wie die Anbieterin) in der DFN-AAI.

Einzelheiten finden Sie auf den Seiten des DFN unter folgender URL:
https://www.aai.dfn.de/der-dienst/

(3) Um die sciebo-Cloud zu nutzen, benötigen Sie eine gültige campusID der TH Köln und das zugehörige Passwort.

(4) Bei Registrierung ihrer Benutzerkennung bei der Anbieterin werden Ihre personenbezogenen Daten an den jeweiligen Dienstanbieter übertragen, verarbeitet und evtl. auch beim Service Provider gespeichert. Diese Daten beinhalten u.a. auch personenbezogene Daten, wie Ihren Vornamen, Nachnamen, die Einrichtung, Ihre dienstliche E-Mailadresse der TH Köln, Ihre campusID und Ihren Status (Studierende*r/Beschäftigte*r).

Weitere Informationen über die Verarbeitung Ihrer personenbezogenen Daten können Sie den Datenschutzinformationen der Anbieterin entnehmen.

Die TH Köln trägt dafür Sorge, dass nur diejenigen personenbezogenen Daten im Rahmen des DFN-AAI herausgegeben werden, die für den Service erforderlich sind.

Passwörter gelangen nicht zu den Service Providern. Die Überprüfung Ihrer campusID und des Passwortes erfolgt immer am Identity Provider der TH Köln. Die gesamte Kommunikation erfolgt dabei ausschließlich verschlüsselt. Die TH Köln übernimmt allerdings keine Verantwortung oder Garantie bzgl. der im Rahmen der DFN-AAI verfügbaren Dienste oder der datenschutzgerechten Nutzung durch den jeweiligen Dienstanbieter.

§ 7 Pflichten der Endnutzer*in

(1) Der/die Endnutzer*in sorgt eigenverantwortlich für die Einhaltung dieser Nutzungsbedingungen und insbesondere der datenschutzrechtlichen, persönlichkeitsrechtlichen, lizenzrechtlichen und urheberrechtlichen Bestimmungen. Eine Nutzung mit rechtswidrigen Inhalten ist unzulässig und bei der Nutzung dürfen keine Rechte (Urheber-, Persönlichkeitsrechte, Vertraulichkeitsvereinbarungen etc.) von Dritten verletzt werden.

(2) Der/die Endnutzer*in trägt dafür Sorge, dass private Daten von den dienstlichen Daten getrennt in unterschiedlichen und entsprechend gekennzeichneten Dateiordnern eingebracht, gespeichert und verarbeitet werden.

(3) Der/die Endnutzer*in ist für die regelmäßige Durchführung und Evaluierung dauerhafter Datensicherungsmaßnahmen gegen Datenverlust der dienstlichen (insbesondere personenbezogenen) Daten verantwortlich und trifft hierzu ggf. geeignete Maßnahmen. Insbesondere ist sicherzustellen, dass regelmäßige Sicherungskopien von den in der sciebo-Cloud gespeicherten Daten erstellt werden und zugriffsgeschützt außerhalb der sciebo-Cloud gespeichert werden und eine regelmäßige Überprüfung der Wiederherstellbarkeit der Sicherungskopien sowie der Wirksamkeit des Datensicherungsverfahrens erfolgt. Bei Nutzung von Dateiverschlüsselung ist zusätzlich das Passwort bzw. der Schlüssel zur Ver- und Entschlüsselung gegen Datenverlust und gegen den Zugriff bzw. die Kenntniserlangung durch unbefugte Dritte zu sichern und außerhalb der sciebo-Cloud sowie getrennt von den verschlüsselten Daten zu verwahren.

(4) Dienstliche, personenbezogene Daten, die in der sciebo-Cloud gespeichert werden, sind grundsätzlich nach Erreichen des Verarbeitungszweckes zu löschen, sofern keine rechtlichen Bestimmungen, z.B. gesetzliche Aufbewahrungsfristen, eine weitere Speicherung erfordern oder erlauben. Der/die Nutzer*in beachtet, dass nach Ende der Vertragslaufzeit oder bei Kündigung des (Endnutzer-) Nutzungsvertrags bzw. bei Auslauf der Nutzungsberechtigung (z.B. bei nicht erfolgter jährlicher Bestätigung der Nutzungsberechtigung) eine Löschung der Daten gemäß § 9 des (Endnutzer-)Nutzungsvertrags „sciebo“ erfolgt und trifft hierzu geeignete Vorkehrungen gegen Datenverlust (z.B. rechtzeitiger Download der Daten.

(5) Zuvor ggf. erteilte Dateifreigabeberechtigungen sind frühestmöglich zu widerrufen, sofern die Dateifreigaben nicht mehr erforderlich sind.

(6) Der/die Endnutzer*in ermittelt vor Auslagerung von dienstlichen, personenbezogenen Daten oder sachbezogenen Daten, die einen hohen Schutzbedarf haben, die Datenkategorie und führt eine Schutzbedarfsanalyse durch. Der hierdurch festgestellte Schutzbedarf legt die zusätzlich zu treffenden organisatorischen und technischen Maßnahmen (wie Datensicherung, Einsatz von Dateiverschlüsselung, Anonymisierung, Pseudonymisierung etc.) fest. Die Feststellung der Maßnahmen hat unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu erfolgen.

§ 8 Sonstiges

Im Übrigen gelten die Bestimmungen der Benutzungsordnung für die zentralen IT-Services der Campus IT, abrufbar unter:

https://www.th-koeln.de/hochschule/ordnungen-der-zentralen-einrichtungen_52256.php