Nutzungsbedingungen für die Verwendung des Cloud-Speicherdienstes „sciebo“ an der FernUniversität in Hagen

Stand:28. November2020

Mit „sciebo“ wird ein datenschutzrechtskonformer Cloud-Speicherdienst zur persönlichen Arbeitserleichterung zur Verfügung gestellt.

„sciebo“ kann im Rahmen der nachfolgenden Nutzungsbedingungen zur Erledigung von dienstlichen Aufgaben verwendet werden und soll nicht verbindlich zugelassene externe Cloud-Speicherdienste ersetzen.

Die Nutzungsbedingungen stellen verbindliche Kriterien für den Nutzerkreis, die Nutzungsszenarien, Art und Umfang der mit „sciebo“ verarbeiteten Daten sowie Art und Weise der Datenverarbeitung auf. **(Zif. I)**

Die Nutzung von „sciebo“ erfolgt auf freiwilliger und eigenverantwortlicher Basis. Jede*r Nutzende ist gehalten, vor der jeweiligen Verwendung des Dienstes eine Vorprüfung bzgl. des beabsichtigten Nutzungsszenarios und der beabsichtigten Datenverarbeitung vorzunehmen.
(Zif. II und III)

Die FernUniversität haftet nicht für Schäden aus dem Verlust oder der Beeinträchtigung von in „sciebo“ abgelegten Daten.

Bei Festlegung der nachfolgenden Nutzungskriterien wurden die speziellen Gegebenheiten des Cloud-Speicherdienstes „sciebo“ berücksichtigt:

- Aufgrund der Vertragskonstruktion von „sciebo“ ist jede*r Endnutzer*in vor Nutzungsbeginn zum Abschluss eines zusätzlichen „Endnutzervertrags“ mit dem Dienstanbieter verpflichtet. Die FernUniversität selbst kann bzw. darf ihre Mitarbeiter*innen und Studierenden hierzu rechtlich nicht verpflichten. Daher erfolgt die Nutzung des Cloud-Speicherdienstes „sciebo“ auf freiwilliger Basis.
- Mangels garantierter Ausfallsicherheit und Backup-Garantie seitens des Diensteanbieters sowie für einen umfassenden Regelbetrieb nicht ausreichend festgelegter Verantwortlichkeiten bezüglich eines Service Licence Agreements und Notfall- und Schwachstellenmanagements handelt es sich bei dem Cloud-Speicherdienstes „sciebo“ um ein nur eingeschränkt rechtssicher nutzbares Tool.

Aus diesen Gründen ist die dienstliche Nutzung von „sciebo“ auf den in den Nutzungsbedingungen beschriebenen Umfang unter den genannten Bedingungen beschränkt.

I. Nutzerkreis, Nutzungszenarien und Kriterien zur Datenverarbeitung bei der Nutzung von „sciebo“

Aufgrund der Vertragskonstruktion von „sciebo“ ist jede*r Endnutzer*in vor Nutzungsbeginn zum Abschluss eines „Endnutzervertrags“ mit dem Dienstanbieter verpflichtet.

1. Nutzerkreis

Gestattet ist eine **freiwillige Nutzung** des Dienstes durch Mitarbeiter*innen der Fakultäten und sonstigen Einrichtungen der FernUniversität im Rahmen der nachfolgenden Nutzungsszenarien und Kriterien zur Datenverarbeitung.

Ebenfalls gestattet ist eine **freiwillige Nutzung** des Dienstes durch Studierende, jedoch ausschließlich zur privaten Organisation ihres Studiums. Eine dienstlich rechtsverbindliche Kommunikation zwischen Mitarbeiter*innen der FernUniversität und Studierenden über „sciebo" ist daher **ausgeschlossen**.

Eine Nutzung des Dienstes für Mitarbeiter*innen in der Zentralen Hochschulverwaltung (ZHV) ist **ausgeschlossen**. Für diese Nutzergruppe ist ein separater Cloud-Speicherdienst in MS Office 365 vorgesehen.

2. Nutzungsszenarien

Zulässig ist eine Nutzung von „sciebo"

- zwecks Datenaustauschs zwischen verschiedenen Arbeitsgeräten zur persönlichen Arbeitserleichterung
- zwecks Datenaustauschs mit Dritten im Kontext von Forschungsvorhaben
- zwecks Datenaustauschs mit Dritten im Kontext von Lehre und Studium **ausschließlich dann**, wenn damit keine rechtsverbindlichen Handlungen verbunden sind und dies nicht an die Einhaltung von Fristen geknüpft ist.
  Ein Austausch von studien- und prüfungsrelevanten Dokumenten zwischen Lehrenden und Studierenden ist **ausgeschlossen.**

3. Besondere Kriterien für die Verarbeitung von Daten in „sciebo"

a) Fehlendes Daten-Backup

Der Diensteanbieter stellt keine serverseitigen Backups der Daten zur Verfügung. Beim Ausfall eines Speicher-Standorts besteht daher das Risiko, dass die in „sciebo" für den Webzugriff oder zur Synchronisation abgelegten Daten zeitweise oder dauerhaft nicht mehr zur Verfügung stehen.
Jede*r Endnutzer*in sorgt eigenverantwortlich für ausreichende anderweitige Datensicherungen. Die FernUniversität haftet nicht für Schäden aus dem Verlust von in „sciebo" abgelegten Daten.

b) Ausreichender Schutz auf den genutzten Endgeräten

Der Zugriff auf die in „sciebo" abgelegten Daten kann mittels einer Clientsoftware oder durch einen Webbrowser erfolgen. Die Clientsoftware hält die Daten auf allen mit einem „sciebo"-Konto verbundenen Geräten synchron. Durch diesen Automatismus kann es schnell passieren, dass evtl. schützenswerte Daten auf unzureichend geschützte Endgeräte gelangen. Dies ist bei der Speicherung der Daten auf „sciebo" zwingend zu beachten.
Jede*r Endnutzer*in hat eigenverantwortlich für einen ausreichenden Schutz der von ihm*ihr verwendeten, mit „sciebo" verbundenen Endgeräte zu sorgen.

c) Einhaltung der datenschutzrechtlichen Vorgaben
Für die in „sciebo“ gespeicherten und verarbeiteten personenbezogenen Daten gelten die Regelungen der Datenschutz-Grundverordnung (DSGVO) und des Datenschutzgesetzes (DSG) NRW.
Jede*r Endnutzer*in ist bei der Nutzung von „sciebo“ für die Einhaltung der Vorschriften der DSGVO und des DSG NRW selbst verantwortlich.
Dies beinhaltet beispielsweise die Prüfung, ob für das Ablegen von Daten auf „sciebo“ eine Einwilligung der/des Betroffenen erforderlich ist.

4. Private Daten

a) Den **Mitarbeiter*Innen** der Fakultäten und sonstigen Einrichtungen der FernUniversität steht „sciebo“ ausschließlich zu dienstlichen Zwecken zur Verfügung; private Daten dürfen dort nicht gespeichert werden.
b) **Studierende** dürfen „sciebo“ zur Speicherung von Daten im Rahmen der persönlichen Organisation ihres Studiums verwenden. Die Ablage von privaten Daten wird seitens der FernUniversität nicht empfohlen, „sciebo“ kann aber zu diesem Zweck genutzt werden.

5. Weitere Hinweise

a) Sparsamer Umgang
Prinzipiell sollte bei der Nutzung von „sciebo“ die Datenmenge gemäß Art. 5 Abs. 1 DSGVO auf das notwendige Mindestmaß begrenzt werden.

b) Sorgfältige Datenübertragung
Bei der Übertragung größerer Datenmengen, beispielsweise ganzer Verzeichnisbäume in die Cloud kann leicht übersehen werden, dass in einem Unterverzeichnis sensible Daten abgelegt wurden, die den Bereich der Einrichtung nicht verlassen dürfen. Jede*r Endnutzer*in ist zu einem entsprechend sorgfältigen Umgang angehalten.

c) Einsatz mit Bedacht
Bevor mithilfe von „sciebo“ Daten auf Endgeräte synchronisiert werden, sollten erwarteter Nutzen und damit verbundene Risiken gegeneinander abgewogen werden.

II. Prüfung der Zulässigkeit der Verarbeitung der einzelnen Datensätze in „sciebo“

Bevor Daten in „sciebo“ abgelegt werden dürfen, sind die nachfolgend erläuterten Abhängigkeiten zwischen der Datenkategorie, dem daraus folgenden Schutzbedarf der Daten und der Eignung zur Ablage in „sciebo“ zu beachten.

Zunächst ist der Schutzbedarf der Daten zu ermitteln. Dafür müssen die Daten in eine der vier vorhandenen Schutzbedarfskategorien („keine“, „normal“, „hoch“ oder „sehr hoch“) eingeordnet werden. Nach ihrer Einordnung in eine der Kategorien lässt sich dann anhand der Schutzbedarfstabelle auf Seite 4 bestimmen, ob eine Ablage der Daten in „sciebo“ zulässig ist oder nicht.

Schutzbedarf bestimmt den Umfang der Cloud-Nutzung

Für die Entscheidung, unter welchen Bedingungen eine Auslagerung von Daten in „sciebo“ in Frage kommt, bildet der Schutzbedarf der Daten die grundlegende Richtschnur. Hinweise auf den Schutzbedarf können bereits aus der Datenkategorie selbst abgeleitet werden. Ergänzt wird dies durch eine systematisch durchgeführte Schutzbedarfsanalyse. Der Schutzbedarf von Daten kann hier mittels der am ISidoR - Security-Audit angelehnten Schutzbedarfsanalyse bestimmt werden (ab Zif III).

Die an der FernUniversität verarbeiteten Daten lassen sich grob in die folgende Kategorienübersicht einteilen:

Kategorienübersicht

Kategorie	**Hinweis auf typischen Schutzbedarf**
Daten aus öffentlich zugänglichen Quellen	keine
Dienstliche (nicht wissenschaftliche) Daten (z.B. Prüfungs-ergebnisse, Gutachten)	Normal bis sehr hoch
Wissenschaftliche Daten (z.B. Untersuchungsergebnisse, vertrauliche Forschungsdaten)	Normal bis 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 können einen sehr hohen Schutzbedarf haben (zum Beispiel auf Grund von Geheimhaltungsvereinbarungen).

Die weitergehende Schutzbedarfsanalyse wird grundsätzlich hinsichtlich der drei Schutzziele *Vertraulichkeit, Integrität* und *Verfügbarkeit* differenziert bestimmt. Entsprechend differenziert sollten Vorkehrungen zur Sicherheit der Daten getroffen werden.

Aus dem Schutzbedarf der Daten folgt zwingend die Eignung oder Nicht-Eignung und damit die Zulässigkeit oder Unzulässigkeit der Speicherung in „sciebo“:

Schutzbedarfstabelle

Schutzbedarf	**Eignung/Zulässigkeit für die Ablage in „sciebo“**
Daten mit keinem oder normalen Schutzbedarf	Ja
Daten mit hohem Schutzbedarf	Nein, da diese nur verschlüsselt gespeichert werden dürften. Dies ist aber kein Standard an der FernUniversität.
Daten mit sehr hohem Schutzbedarf	Nein

III. Schutzbedarfsanalyse - ISidoR - Security-Audit

Aus dem Schutzbedarf der für eine Speicherung vorgesehenen Daten folgt nicht nur, ob eine Speicherung zulässig ist oder nicht, sondern auch unter welchen Bedingungen dies geschehen kann. Dabei ist der Schutzbedarf nach den drei Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit zu betrachten. Auf „sciebo" bezogen bedeuten sie folgendes:

Verfügbarkeit
Die Daten in „sciebo" befinden sich an einem von drei Standorten in NRW. Es gibt keine serverseitigen Backups der Daten. Beim Ausfall eines Standorts könnten die Daten daher zeitweise oder dauerhaft nicht für den Webzugriff oder zur Synchronisation zur Verfügung stehen. Die FernUniversität haftet nicht für Schäden aus dem Verlust von Daten. Der*die Endnutzer*in ist für Datensicherungen selbst verantwortlich. **Wenn sehr hohe Anforderungen an die Verfügbarkeit gestellt werden, ist eine Datenablage in „sciebo" unzulässig.**

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 „sciebo" eine größere Angriffsfläche als Dienste, die ausschließlich FernUniversitätsintern 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 der*die 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.

Vertraulichkeit
Die Einhaltung der Datenschutzvorschriften wird durch die beteiligten Hochschulen sichergestellt. Insbesondere werden Daten nicht an Privatunternehmen weitergegeben, nicht durch diese verarbeitet und auch nicht außerhalb des Gebietes der Bundesrepublik Deutschland abgespeichert. „sciebo" bietet allerdings eine größere Angriffsfläche als ein nur FernUniversitätsintern angebotener Dienst. 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 zwingend notwendig. Es wird keine serverseitige Verschlüsselung angeboten, da diese keinen ausreichenden Schutz bietet. Darum sollte die Verschlüsselung selbst 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 sie nach allgemein anerkannten Regeln als sicher gilt.

Durchführung der Schutzbedarfsanalyse/Schutzbedarfskategorien

Anhand der folgenden Übersichten ist der Schutzbedarf der betreuten Daten festzustellen.
Die Übersichten sind angelehnt an die Richtlinien zum IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI). Die Schutzbedarfsanalyse kann hier mit dem Security-Audit ISidoR durchgeführt werden.

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 Informations-Versorgungs-Sicherheit

(Verfügbarkeit, Integrität, Vertraulichkeit) verletzt wird. Dabei ergibt sich der Schutzbedarf aus den unmittelbaren Schäden und durch die möglichen Folgeschäden (z.B. Schadensersatzforderungen, Produktionsausfallkosten, etc.). Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts stellt dabei immer einen Datenschutzverstoß dar.

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 Schutzzielen:

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

Schutzbedarfskategorie: „Keine“

Schäden haben nur eine unwesentliche Beeinträchtigung der Institution oder anderer an „sciebo“ 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 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 zwei Tagen.

Schutzbedarfskategorie: „Normal“

Schäden haben Beeinträchtigungen der Institution oder anderer an „sciebo“ 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. Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse 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.

Schutzbedarfskategorie: „Hoch“

Im Schadensfall tritt Handlungsunfähigkeit wichtiger Bereiche der Institution oder anderer an „sciebo“ teilnehmenden Institutionen ein; Schäden haben erhebliche Beeinträchtigungen der Institution selbst, anderer an „sciebo“ 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 Vertrauens-beeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Verfügbarkeit der Daten

Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen bei bis zu 4 Stunden.

Schutzbedarfskategorie: „Sehr hoch“

Der Schadensfall kann zum totalen Zusammenbruch der Institution oder anderer an „sciebo“ teilnehmenden Institutionen führen, 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.