**Stand: 11. Februar 2020**

# Nutzungsbedingungen für die Verwendung des Cloudspeicherdienstes „sciebo“ an der FernUniversität in Hagen

## *I. Festlegung des Nutzerkreises, der Datenkategorien und des Umfangs der Datenmenge für die Nutzung von „sciebo“*

## *Allgemeine Kriterien für die Verarbeitung von Daten in „sciebo“*

Diese Nutzungsbedingungen stellen verbindliche Kriterien dafür auf, welche Daten von welchen Mitgliedern und Angehörigen der FernUniversität in Hagen in „sciebo“ verarbeitet werden dürfen und welche nicht. Berücksichtigt werden die speziellen Gegebenheiten des „sciebo“ genannten Cloudspeicherdienstes.

## *Freiwillige Nutzung; Ausschluss der Nutzung externer Repositories*

„Sciebo“ wird als freiwillig nutzbare, jedoch nicht verpflichtend zu nutzende Speichermöglichkeit an der FernUniversität in Hagen eingeführt. Hintergrund für diese Einschränkung ist, dass aufgrund der Vertragskonstruktion von „sciebo“ die EndnutzerInnen vor Beginn der Nutzung noch einen Nutzungsvertrag mit sciebo abschließen müssen. Hierzu können die Mitglieder und Angehörigen der FernUniversität von dieser jedoch nicht verpflichtet werden. Bei Studierenden kommt noch folgendes hinzu: Hinsichtlich „Moodle“, werden die Studierenden über § 12a ZEO verpflichtet, diese Lehr- / Lernumgebung in dem von den Fakultäten jeweils verbindlich festgelegten Umfang zu nutzen. Eine entsprechende Regelung für die verbindliche Nutzung von „sciebo“ existiert nicht. Dies bedeutet, dass Studierende aktuell nicht verpflichtet werden können, Prüfungsleistungen mittels „sciebo“ auszutauschen. Ein Datenaustausch kann z. B. weiterhin per Mail erfolgen. Prüfungsleistungen können über die Lernplattform Moodle bereitgestellt werden. Trotz der Freiwilligkeit der Nutzung von „sciebo“, ist die Nutzung externer Repositories wie z. B. Google Drive oder Dropbox zum Datenaustausch mit der Einführung des Dienstes „sciebo“ an der FernUniversität nicht mehr zulässig. Mit „sciebo“ wird ein datenschutz- und rechtskonformer Cloud-Speicherdienst zur Verfügung gestellt, der kostenlos genutzt werden kann.

## *Nutzung ausschließlich zu Zwecken von Forschung, Lehre und Studium und damit nicht zu Verwaltungszwecken*

Der Dienst „sciebo“ darf nur zu Zwecken von Forschung, Lehre und Studium und damit nicht zu Verwaltungszwecken genutzt werden. Weiterhin wird sciebo als rein **freiwillig und eigenverantwortlich** nutzbares Tool zur persönlichen Arbeitserleichterung zur Verfügung gestellt. Eine verpflichtende Nutzung von „sciebo“ für Verwaltung sowie studien- und prüfungsrelevante Leistungen in Lehre und Studium kann nicht erfolgen. Auch ein studien- und prüfungsrelevanter, verbindlicher Austausch zwischen Lehrenden und Studierenden ist ausgeschlossen. Mangels Ausfallsicherheit, Backup und klarem Vertragskonstrukt hinsichtlich eines Service Licence Agreements, Notfall- und Schwachstellenmanagements handelt es sich bei dem durch den Konsortialführer bereitgestellten Tool um kein rechtssicheres Tool.
Eine **freiwillige Nutzung** des Dienstes durch Wissenschaftliche Mitarbeiter*Innen, in der Lehre tätigen Personen und Studierende im o.g. Sinne ist somit gestattet. Eine Nutzung für Mitarbeiter*Innen in der ZHV wird **ausgeschlossen**.
Die Begründung für den Ausschluss der Nutzung durch Mitarbeiter*Innen der ZHV lautet:

a) Mit der Einführung von Office 365 steht den Mitarbeiter*Innen der ZHV zukünftig ein Tool für die Speicherung von Daten in der Cloud zur Verfügung. Ein weiteres vergleichbares Instrument ist damit nicht erforderlich.
b) Die Daten, die in sciebo abgespeichert werden, stehen unter einem permanenten Ausfallrisiko. Daher sind sie als verlässliche Datenquelle für die ZHV nicht geeignet.

c) Sciebo ist als Medium für den Austausch von Daten zwischen Forscher*Innen und Studierenden unterschiedlicher Hochschulen in NRW vorgesehen. Bei Daten aus der ZHV ist dies nicht der Fall.

Die Festlegung dieser Nutzungsmöglichkeiten erfolgt über § 2 des Nutzungsvertrags. Danach legt die Heimateinrichtung fest, welche dienstlichen Daten in „sciebo" verarbeitet werden dürfen. Die FernUniversität sieht die Verarbeitung von dienstlichen Daten bis zur Einführung von Office 365 ausschließlich in physischen Speicherungsmöglichkeiten vor.
Eine verpflichtende Nutzung für Verwaltung und Studien- und prüfungsrelevanten Leistungen in der Lehre von „sciebo" kann nicht erfolgen. Mangels Ausfallsicherheit, Backup und klarem Vertragskonstrukt hinsichtlich eines Service Licence Agreements, Notfall- und Schwachstellenmanagements handelt es sich bei dem durch den Konsortialführer bereitgestellten Tool um kein rechtssicheres Tool.

## *Besondere Kriterien für die Verarbeitung von Daten in „sciebo"; keine Backups von Daten*

Unter dem Gesichtspunkt des Erfordernisses der Verfügbarkeit von Daten, sind bei der Verarbeitung von Daten in „sciebo" folgende Überlegungen mit einzubeziehen: Die in „sciebo" gespeicherten Daten befinden sich auf Servern der WWU in Münster oder ihrer Kooperationspartner in Bonn und Duisburg-Essen. Für die dortige Speicherung und Verarbeitung personenbezogener Daten gelten daher die DSGVO und das DSG 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 Endnutzer ist für Datensicherungen selbst verantwortlich. Der Zugriff auf die Daten kann mittels einer Clientsoftware oder durch einen Webbrowser erfolgen. Die Clientsoftware hält die Daten auf allen mit einem „sciebo"-Konto verbundenen Geräten synchron. Dadurch passiert es schnell, das evtl. schützenswerte Daten auf unzureichend geschützte Endgeräte gelangen. Dies ist bei der Speicherung der Daten auf „sciebo" unbedingt zu beachten und zu unterlassen. Der Nutzungsvertrag zwischen „sciebo" und den Endnutzerinnen enthält hinsichtlich der Speicherung personenbezogener Daten Dritter in § 6 Absatz 2 die Bestimmung, „…, dass Nutzer als ggf. verantwortliche Stelle im Sinne des Datenschutzrechtes dafür Sorge zu tragen haben, dass die Verarbeitung der Daten in Einklang mit dem geltenden Datenschutzrecht steht." Das bedeutet, dass die Verarbeitung der personenbezogenen Daten rechtmäßig im Sinne von Art. 6 DSGVO erfolgen muss, also beispielsweise eine Einwilligung des Betroffenen zur Verarbeitung vorliegt oder die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Für die Erfüllung dieser Voraussetzungen sind wiederum die EndnutzerInnen verantwortlich.

## *Private Daten*

Hinsichtlich der Nutzung von „sciebo" für die Verarbeitung von privaten Daten gilt folgendes:

a) Studierende: 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.
b) Beschäftigte: Den Beschäftigten in Forschung und Lehre steht „sciebo" zu dienstlichen Zwecken zur Verfügung; private Daten dürfen dort nicht gespeichert werden.

## *Sparsamer Umgang*

Prinzipiell sollte bei der Nutzung von „sciebo" 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 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 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 3 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. Der Schutzbedarf von Daten kann hier mittels der am ISidoR - Security-Audit angelehnten Schutzbedarfsanalyse bestimmt werden (ab Seite 4).

Hinweise auf den Schutzbedarf können zum einen aus der systematisch durchgeführten Schutzbedarfsanalyse und zum anderen aus der Datenkategorie abgeleitet werden. 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).

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 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 nur verschlüsselt; dies ist aber kein Standard an der FernUni |

| | |
|---|---|
| Daten mit sehr hohem Schutzbedarf | nein |

## 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 Verfügbarkeit, Integrität und Vertraulichkeit 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 Endnutzer 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 FernUniveristäts intern 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 Nutzer 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 FernUniversitäts intern 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.

Anhand der folgenden Übersichten soll der Schutzbedarf der betreuten Daten festgestellt werden.

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 auf-
zustellen, 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.<br>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.<br>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.<br>Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen |
| **Beeinträchtigung des informationellen Selbstbestimmungsrechts** | Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als tolerabel eingeschätzt.<br>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.<br>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.<br>Vertragsverletzungen mit hohen Konventionalstrafen. |
| **Beeinträchtigung des informationellen Selbstbestimmungsrechts** | Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich.<br>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.<br>Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen bei bis zu 4 Stunden. |

## *Schutzbedarfskategorie: „Sehr hoch“*

Der Schadensfall führt zum totalen Zusammenbruch der Institution oder anderer an „sciebo“ 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.<br>Vertragsverletzungen, deren Haftungsschäden ruinös sind. |
| **Beeinträchtigung des informationellen Selbstbestimmungsrechts** | Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich.<br>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.<br>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.<br>Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen unter einer Stunde. |