UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Richtlinie zur Nutzung von Sciebo

Bereich / Projekt:	Informationssicherheit
Autor(en):	AG IT-Sicherheit, Vorfallteam
Dateiablage:	Sciebo
Version / Stand:	Version 1.0, 2.7.2020

1 Einleitung

Sciebo ist ein Cloud-Speicherdienst in NRW, der von Hochschulen für Hochschulen betrieben und vom Land NRW finanziell gefördert wird. Der Dienst erlaubt es allen Mitarbeiter*innen und Student*innen der teilnehmenden Hochschulen Daten in Sciebo zu verarbeiten (bspw. speichern, verändern, teilen, hoch- und runterladen). Mit Hilfe von Software auf Desktop- und Mobilgeräten können zudem die auf unterschiedlichen Geräten gespeicherten Dateien automatisiert synchronisiert werden. Darüber hinaus besteht die Möglichkeit, mit allen üblichen Webbrowsern auf die Daten zuzugreifen. Weiter erlaubt es Sciebo, gespeicherte Dateien mit anderen Nutzer*innen von Sciebo in Sciebo und darüber hinaus auch mit beliebigen anderen Personen über einen Link zu teilen.

2 Geltungsbereich

Diese Richtlinie regelt die dienstliche Nutzung von Sciebo und die damit verbundene Verarbeitung von Daten der Universität. Sie hat verbindliche Gültigkeit für alle Mitarbeiter*innen der UPB.

3 Zielsetzung

Ziel dieses Dokuments ist es, verbindliche Regeln für die Nutzung von Sciebo an der UPB festzulegen. Durch diese wird sichergestellt, dass die UPB sowie betroffenen Personen durch die Nutzung von Sciebo keinen unnötigen Risiken ausgesetzt werden. Dazu wird insbesondere geregelt, unter welchen Umständen eine Datei in Sciebo gespeichert werden darf. Darüber hinaus werden allgemeine Verhaltensweisen im Umgang mit Sciebo in folgenden Abschnitt festgelegt.

4 Allgemeine Verhaltensweisen im Umgang mit Sciebo

Neben der Auswahl der Daten, die in Sciebo verarbeitet werden dürfen, sind weitere Verhaltensgrundsätze zu berücksichtigen, die in den folgenden beiden Unterabschnitten festgelegt sind.

4.1 Erlaubte Nutzung

Die Nutzung von Sciebo ist gemäß den Nutzungsbedingungen des Dienstes nur zu Zwecken von Studium, Lehre, Forschung und Verwaltung erlaubt.

Personenbezogene Daten dürfen in Sciebo gemäß DS-GVO nur dann verarbeitet werden, wenn für die Verarbeitung eine tragfähige Rechtsgrundlage (Zulässigkeit der Verarbeitung) und die Gewährleistung der Sicherheit der Datenverarbeitung gegeben ist. Es gelten die Verarbeitungsgrundsätze gemäß Art. 5 DS-GVO und die Bedingungen für die Rechtmäßigkeit der Verarbeitung gemäß Art. 6 DS-GVO. Zur Eindämmung von Risiken für die Rechte und Freiheiten der von einer Verarbeitung Betroffener sind bezüglich der Verarbeitung geeignete technische und organisatorische Maßnahmen umzusetzen (Art. 25 Abs. 1 und 32 Abs. 1 DS-GVO). Die Auswahl geeigneter Maßnahmen ist abhängig von den im Einzelfall bestehenden Risiken. Personenbezogene Daten mit sehr hohem Schutzbedarf (bspw. Gesundheitsdaten) dürfen gemäß Art. 9 Abs.1 DS-GVO nicht in Sciebo verarbeitet werden.

4.2 Vor der Verarbeitung die Konsequenzen überprüfen

Es ist leicht, in Sciebo gespeicherte Daten mit weiteren Personen zu teilen und Dateien gegebenenfalls automatisch auf weitere Geräte zu übertragen. Vor der Speicherung von Daten in Sciebo sind daher immer zuerst die Konsequenzen der Verarbeitung zu bedenken, insbesondere, an welche weiteren Personen und auf welche Geräte die Daten automatisch übertragen werden.

5 Geeignete Dateien für Sciebo

Um zu entscheiden, ob eine Datei in Sciebo verarbeitet werden darf und welche zusätzlichen Schutzmaßnahmen gegebenenfalls getroffen werden müssen, werden Informationen in den Dateien entsprechend ihres Schutzbedarfs

bezüglich der Schutzziele Vertraulichkeit und Integrität jeweils in die Kategorien „Normaler Schutzbedarf“, „Hoher Schutzbedarf“ und „Sehr hoher Schutzbedarf“ eingeordnet.

Der Schutzbedarf der Verfügbarkeit wird nicht beurteilt, da die Speicherung einer Datei in Sciebo sich wie in 6.2 beschrieben weder entscheidend positiv noch negativ auf die Verfügbarkeit der Datei auswirkt.

Um diese Einordnung zu treffen, nehmen Sie bitte die „Richtlinie zur Einordnung des Schutzbedarfs von Informationen“ zur Hand. Oftmals können Sie den Schutzbedarf auch vereinfacht mit der Liste „Klassen von Informationen und ihr üblicher Schutzbedarf“ bestimmen.

Eine Verarbeitung von Datei in Sciebo ist ohne Einschränkung erlaubt, wenn der Schutzbedarf normal ist. Sie ist nicht erlaubt, wenn der Schutzbedarf als sehr hoch zu klassifizieren ist. Bei hohem Schutzbedarf müssen bei der Verarbeitung die unter 6 beschriebenen zusätzlichen Schutzmaßnahmen getroffen werden.

	Normaler Schutzbedarf	Hoher Schutzbedarf	Sehr Hoher Schutzbedarf
Vertraulichkeit	Erlaubt	Nur mit den in 6 beschriebenen Schutzmaßnahmen erlaubt	Nicht erlaubt
Integrität	Erlaubt	Nur mit den in 6 beschriebenen Schutzmaßnahmen erlaubt	Nicht erlaubt

6 Technische Grenzen von Sciebo

Die Betreiber von Sciebo bemühen sich darum, die oben beschriebenen Schutzziele für die Dateien von Nutzer*innen zu gewährleisten. Dennoch kann die Einhaltung der Schutzziele bei einem hohen oder sehr hohen Schutzbedarf nicht garantiert werden. Solche Dateien dürfen daher gar bzw. nur unter den in den folgenden Abschnitten beschriebenen zusätzlichen Anforderungen und mit den folgenden Maßnahmen verarbeitet werden

6.1 Vertraulichkeit und Integrität sicherstellen

Da Sciebo weder die Vertraulichkeit noch die Integrität von gespeicherten Dateien sicherstellt, müssen Sie vor der Speicherung von Dateien mit hohem Schutzbedarf selber Maßnahmen ergreifen.

Um die Vertraulichkeit von Dateien sicherzustellen, müssen Sie diese vor der Speicherung in Sciebo mit einer dafür geeigneten Software verschlüsseln. Hilfe bei der Auswahl geeigneter Software zur Verschlüsselung von Dateien finden Sie auf den Hilfeseiten des IMT zum Thema „Dateiverschlüsselung einsetzen“.

Integrität von Dateien kann ebenfalls durch geeignete Software zur Dateiverschlüsselung sichergestellt werden. Zur Gewährleistung der Integrität können Sie daher auch den Hilfestellungen auf den Hilfeseiten des IMT zum Thema „Dateiverschlüsselung einsetzen“ folgen.

6.2 Verfügbarkeit sicherstellen

Für die dauerhafte Verfügbarkeit von Dateien gibt es in Sciebo keine Garantie, auch ein Schutz vor versehentlichem Löschen ist nicht vorhanden. Als Mitarbeiter*innen der UPB bedeutet dies, dass Sie die Verfügbarkeit von Dateien selbst sicherstellen müssen. Hilfe hierbei finden Sie auf den Hilfeseiten des IMT zum Thema „Daten sicher aufbewahren“.

6.3 Datenminimierung, Nichtverkettung, Transparenz und Intervenierbarkeit sicherstellen

Sofern personenbezogene Daten Gegenstand von Informationen sind, sind ferner die weiteren datenschutzrechtlichen Anforderungen zu beachten, namentlich die Datenminimierung (Daten werden nur

beschränkt auf das notwendige Maß verarbeitet), die Nichtverkettung (Daten, die zu unterschiedlichen Zwecken verarbeitet werden, dürfen nicht zusammengeführt werden), die Transparenz (Erkennbarkeit, wer Daten von wem zu welchem Zweck, durch welche Systeme und auf welche Art und Weise verarbeitet) sowie die Intervenierbarkeit (Sicherstellung der Betroffenenrechte (z. B. Auskunft gemäß Art. 15 DS-GVO und ggf. Umsetzung von erforderlichen Maßnahmen)). Diese Anforderungen müssen Nutzer*innen selbst sicherstellen. Alle Nutzer*innen können Beratung zur Bestimmung individueller datenschutzrechtlicher Risiken bei der behördlichen Datenschutzbeauftragten der UPB in Anspruch zu nehmen.

7 Weitere Informationen

Weitere Informationen finden Sie

- unter www.sciebo.de und www.sciebo.de/agb zu Sciebo
- unter hilfe.upb.de zum Thema Sciebo, Dateiverschlüsselung und Datensicherung
- unter www.upb.de/datenschutz zum Umgang mit datenschutzrechtlichen Risiken
- unter www.upb.de/informationssicherheit zu Schutzbedarfen von Informationen und Daten