Datenkategorien und ihre Eignung zur sciebo-Cloud-Nutzung

Bei der Nutzung von sciebo muss darauf geachtet werden, dass keine Rechte von Dritten verletzt werden. Das vorliegende Dokument dient als Richtlinie, um zu entscheiden ob, und wenn ja, wie Sie sciebo zum verwalten ihrer Daten nutzen können.

Natürlich ist das Abrufen, Anbieten, Hochladen oder Verbreiten von rechtswidrigen Inhalten, insbesondere solchen, die gegen strafrechtliche, datenschutzrechtliche, persönlichkeits-rechtliche, lizenzrechtliche, oder urheberrechtliche Bestimmungen verstoßen, generell unzulässig. In vielen Fällen ist allerdings eine grobe Einschätzung des Risikos das mit einem möglichen Datenverlust/Verlust der Vertraulichkeit einhergeht, notwendig, um zu entscheiden ob sciebo genutzt werden kann, und gegebenenfalls mit welchen Einschränkungen. Aus der vorliegenden Tabelle können Sie typische Schutzbedarfe für übliche Datenkategorien ablesen. Die Maßnahmen die bei den verschiedenen Schutzstufen getroffen werden sollten, finden Sie weiter unten.

Kategorie	Hinweis auf typischen Schutzbedarf
Daten, die aus öffentlichen und für jeden frei und offenkundig legal zugänglichen Quellen stammen (z.B. Literatur, Dokumente oder Downloads)	Keinen
Daten zu Prüfungen (z.B. Gutachten, Notenlisten)	Hoch (Prüfungsdaten wie Noten dürfen nur einem eingeschränkten, berechtigten Kreis zugänglich gemacht werden)
Daten zu Lehrveranstaltungen (z.B. Teilnehmendenlisten)	Normal (Dies gilt auch, wenn statt Namen nur Matrikelnummern benutzt werden)
Fotos & Videos von üblichen Veranstaltungen ohne sensiblen Inhalt und ohne dass eine einzelne Person oder kleine Gruppe klar erkennbar in den Vordergrund gestellt ist (z.B. von öffentliche Veranstaltungen, Abschlussfeiern..)	Normal
Video- & Audioaufnahmen von Interviews (ohne besondere Inhalte, die einem noch höheren Schutzbedarf zuzuordnen wären)	Hoch
Handgeschriebene Texte (in Kombination mit Namen oder Matrikelnr.)	Hoch
Projektakten (z.B. Arbeitspaketbeschreibungen, Abschlussberichte..)	Normal
Biometrische Daten (Augenablichtungen, Fingerabdruckscans)	Sehr Hoch
Wissenschaftliche Daten (z.B. Geodaten, Mobile Verkehrsdaten, Untersuchungs-ergebnisse, Patientendaten, Messreihen)	Hoch

Wissenschaftliche Daten, sofern sie für Dritte nicht interpretierbar sind	Normal
Daten zu Beschäftigungsverhältnissen	Normal
Besondere sachliche Verhältnisse von Beschäftigten	Sehr Hoch
Daten mit Gesundheitsbezug	Sehr hoch
Daten zu rassisch/ethnischer Herkunft, politischen Meinungen, Gewerkschaftszugehörigkeit, Sexueller Orientierung,	Sehr hoch
Daten zu sozialen Verhältnissen	Hoch

In jedem Fall sind die folgenden Aspekte zu beachten:
Für personenbezogene Daten (sowohl mit dienstlichem als auch privatem Bezug) gelten die Bestimmungen des Datenschutzes. Auch Daten ohne Personenbezug können einen sehr hohen Schutzbedarf haben (zum Beispiel auf Grund von Geheimhaltungsvereinbarungen) oder weil andere rechtliche oder Vertraulichkeitsrisiken bestehen.

Ein Schutzbedarf im Einzelfall wird grundsätzlich hinsichtlich der möglichen Gefahren für Betroffene, die Hochschule und Dritte (Projektpartner) bestimmt. Entsprechend dieser Gefahren sind die drei Informationssicherheitsschutzziele Verfügbarkeit, Integrität und Vertraulichkeit jeweils differenziert zu betrachten. Entsprechend differenziert müssen Vorkehrungen zur Sicherheit der Daten getroffen werden. Im Zweifel fragen Sie nach (Datenschutzbeauftragte, Beauftragte der Informationssicherheit)
Aus dem Schutzbedarf der Daten folgt zwingend die Eignung oder Nicht-Eignung zur Speicherung in sciebo. Im Falle von mehreren in Frage kommenden Kategorien ist die mit dem jeweils höchsten Schutzbedarf zu wählen. Die vorliegenden Überlegungen lassen sich nicht ohne weiteres auf andere Cloudspeicherdienste übertragen, weil hinsichtlich sciebo besondere vertragliche und praktische Konstellation in die Beurteilung eingeflossen sind.

Schutzbedarf	Eignung
Daten, mit keinem Schutzbedarf	Für die Ablage geeignet
Daten mit normalen Schutzbedarf	Für die Ablage geeignet, auch hier wird die Verschlüsselung empfohlen
Daten mit hohem Schutzbedarf	Nur für die verschlüsselte Ablage geeignet
Daten mit sehr hohem Schutzbedarf	Nicht für die Ablage geeignet

Insbesondere dürfen die folgenden Daten nicht in der Cloud abgelegt werden

Schutzbedarf	Eignung
• Personalaktendaten/ besondere sachliche Verhältnisse von Beschäftigten	Nicht für die Ablage geeignet
• Sensible personenbezogene Daten (Gesundheitsbezug, rassisch/ ethnische Herkunft, politische Meinungen, Gewerkschafts-zugehörigkeit, Sexuelle Orientierung, Biometrische Daten, besondere sachliche Verhältnisse)	Nicht für die Ablage geeignet
• Haushaltsdaten	Nicht für die Ablage geeignet