



## Handreichung zum sicheren und datenschutzkonformen Umgang mit Citavi an der Universität

Version: 1.0  
Datum: 11. März 2024  
Klassifizierung: NICHT-ÖFFENTLICH  
Status: in Arbeit / vorgelegt / **freigegeben**  
Autor: Sebastian Zimmermann  
Verteiler: Forschende, Lehrende und Studierende

### Einleitung

Citavi ist ein wertvolles Werkzeug für die Literaturverwaltung und Wissensorganisation. Diese Handreichung bietet praktische Tipps, um Citavi sicher zu nutzen und dabei den Datenschutz zu wahren.

### Einfache Schritte für eine sichere Nutzung von Citavi

**Installation:** Laden Sie Citavi nur unter diesem [Link](#) herunter und installieren Sie es auf Geräten, die durch aktuelle Antivirensoftware geschützt sind.

**Updates:** Aktualisieren Sie Citavi regelmäßig, um von den neuesten Sicherheitsfeatures zu profitieren.

**Zugriffskontrolle:** Vergeben Sie Zugriffsrechte sorgfältig und nur an Personen, die unmittelbar an Ihrem Projekt beteiligt sind.

**Backups:** Erstellen Sie regelmäßige Backups Ihrer Projekte auf externen Speichermedien oder verschlüsselten Cloud-Services. [Hier](#) finden Sie Hinweise, welche Möglichkeiten Ihnen zur Verfügung stehen.

Bitte lassen Sie sich bei Bedarf bei den Ansprechpartnern des ZIMT-Support beraten (support@zimt.uni-siegen.de)

### Datenschutz im Fokus

**Vermeidung personenbezogener Daten:** Speichern Sie **keine Forschungsdaten** und **keine personenbezogenen Daten** in der Citavi Cloud. Hierfür stehen aktuell bereichsbezogene NAS-Laufwerke zur Verfügung. Sollen die Daten mit Personen außerhalb der Universität Siegen



geteilt werden, kann auch SharePoint genutzt werden. Beide Dienste stehen über das ZIMT zur Verfügung.

**Anonymisierung:** Entfernen oder verfremden Sie Identifikationsmerkmale aus Ihren Daten.

## Umgang mit sensiblen Forschungsdaten

**Vertraulichkeit:** Behandeln Sie alle Daten vertraulich, insbesondere wenn sie sensible Informationen enthalten.

**Auch hier gilt:** Speichern Sie keine Forschungs- oder personenbezogenen Daten in der Citavi-Cloud! Hierfür stehen aktuell bereichsbezogene NAS-Laufwerke zur Verfügung. Sollen die Daten mit Personen außerhalb der Universität Siegen geteilt werden, kann auch SharePoint genutzt werden. Beide Dienste stehen über das ZIMT zur Verfügung.

Nichtveröffentlichte Forschungsdaten gelten grundsätzlich mindestens als vertraulich!

**Klassifizierung:** Ordnen Sie Ihre Daten nach Vertraulichkeit ein: (öffentlich, nicht-öffentlich, vertraulich und streng-vertraulich). Weitere Hinweise zur Klassifizierung Ihrer Daten finden Sie [hier](#).

**Berechtigungen:** Stellen Sie sicher, dass nur berechtigte Teammitglieder Zugang zu sensiblen Daten haben.

## Praktische Anwendungstipps

**Cloud-Nutzung:** Wählen Sie Cloud-Dienste mit Sitz in der EU für die Synchronisation Ihrer Datenbank aus Datenschutzgründen. Verwenden Sie vorzugsweise vom ZIMT bereitgestellte Systeme, da diese bereits durch die Informationssicherheit und den Datenschutz der Uni Siegen geprüft wurden.

**Teamarbeit:** Nutzen Sie Teamfunktionen für gemeinsame Projekte und achten Sie auf entsprechende Berechtigungsrollen der Personen.

**Verschlüsselung nutzen:** Verschlüsseln Sie Ihre Daten sowohl bei der Übertragung als auch bei der Speicherung. Dies gilt auch und insbesondere für Sciebo.

Sollten weitere Informationen benötigt werden, dann schauen Sie gerne in die Handreichung zur Verschlüsselung.

Bitte lassen Sie sich bei Bedarf bei den Ansprechpartnern des ZIMT-Support beraten!

## Rechtliche Rahmenbedingungen beachten

**DSGVO-Konformität prüfen:** Vergewissern Sie sich, dass Ihre Arbeit mit Citavi im Einklang mit der DSGVO steht.

**Nationale Gesetze berücksichtigen:** Beachten Sie zusätzlich nationale Datenschutzgesetze sowie die Richtlinien Ihrer Universität.



## Checkliste für den Alltag

- Offizielle Quelle für Download und Installation von Citavi genutzt?
- Regelmäßige Updates durchgeführt?
- Zugriffsrechte überprüft und angepasst?
- Backup der Citavi-Datenbank erstellt?
- VVT durchgeführt bei Verarbeitung personenbezogener Daten?

Bei Fragen oder Unsicherheiten wenden Sie sich bitte an das Team der Stabsstelle Informationssicherheit und Datenschutz

[datenschutz@uni-siegen.de](mailto:datenschutz@uni-siegen.de)  
[ciso-team@uni-siegen.de](mailto:ciso-team@uni-siegen.de)