UNIVERSITÄT SIEGEN

Amtliche Mitteilungen

Datum **20. Juli 2020** **Nr. 41/2020**

I n h a l t :

Richtlinie zur Nutzung von Meeting-Systemen und Cloud-Diensten an der Universität Siegen

Vom 16. Juli 2020

Herausgeber: Rektorat der Universität Siegen
Redaktion: Dezernat 3, Adolf-Reichwein-Straße 2 a, 57076 Siegen, Tel. 0271/740-4813

Richtlinie
zur Nutzung von
Meeting-Systemen und Cloud-Diensten
an der
Universität Siegen

Vom 16. Juli 2020

Inhaltsverzeichnis

1. Zweck und Geltungsbereich

Im Rahmen dieser Richtlinie werden verbindliche Regelungen zum dienstlichen Umgang mit Meeting-Systemen und Cloud-Diensten an der Universität Siegen getroffen.

Durch die Nutzung von Meeting-Systemen und Cloud-Diensten entsteht ein erhöhtes Risiko bezüglich der Verletzung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit und damit einhergehend auch bezüglich der Verletzung rechtlicher Vorgaben zum Datenschutz (EU-DSGVO und DSG-NRW). Gründe dafür können z.B. Unklarheit über Zugriffsrechte Dritter, der oft unbekannte Speicherort der Daten und meist ungeregelte Zuständigkeiten, beispielsweise bei Verlust oder Löschung von Daten, sein.

Diese Richtlinie gilt verbindlich für alle Mitglieder und Angehörige der Universität Siegen, in Bezug auf die dienstliche Verarbeitung und Speicherung von Daten und Informationen im Zusammenhang mit Meeting-Systemen und Cloud-Diensten.

Für die Umsetzung dieser Richtlinie sind die Hochschulleitung, die Dekaninnen und Dekane der Fakultäten, die Hochschullehrerinnen und Hochschullehrer, die Leiterinnen und Leiter der zentralen Einrichtungen und Betriebseinheiten, Referatsleiterinnen und Referatsleiter sowie die Dezernentinnen und Dezernenten der Universitätsverwaltung und in der konkreten Anwendung die Nutzerinnen und Nutzer der Universität Siegen verantwortlich.

2. Abgrenzung und Begriffsdefinition

Die vorliegende Richtlinie bezieht sich auf die temporäre und längerfristige Überlassung von Daten an einen Cloud-Dienstanbieter und insbesondere auf die Nutzung von

- **Meeting-Systemen** im Sinne von *Videokonferenzsystemen*, *Telefonkonferenzsystemen* und *Chatsystemen*, mit denen mit internen und externen Kommunikationspartnerinnen und Kommunikationspartnern via Text, Ton, Bild oder über die Freigabe von Bildschirminhalten oder Präsentationen Informationen ausgetauscht werden können.
- **Cloud-Diensten** im Sinne von IT-Infrastrukturen, die sowohl eine temporäre als auch längerfristige Speicherung von Daten, auf die unabhängig von Ort und Zeit über ein Kommunikationsnetz zugegriffen werden kann, ermöglichen, unabhängig von der Cloud-Artikel

3. Regelungen

Im Folgenden werden Regelungen zur Speicherung und Verarbeitung dienstlicher Daten mit Meeting-Systemen und Cloud-Diensten aufgelistet.

3.1 Nutzung von Meeting-Systemen und Cloud-Diensten

Die Universität Siegen stellt ihren Mitgliedern Meeting-Systeme und Cloud-Dienste für die dienstliche Nutzung zur Verfügung. Zur Erhebung, Verarbeitung und Speicherung dienstlicher Daten innerhalb von Meeting-Systemen und Clouddiensten sind diese, durch das Zentrum für Informations- und Medientechnologie (ZIMT) der Universität Siegen bereitgestellten Dienste und Lizenzen unter Beachtung der jeweiligen Nutzungsbedingungen zu nutzen[1].

Dienste, die lokal im ZIMT der Universität betrieben werden, sind, wenn technisch möglich, zu bevorzugen.

Die Nutzung von nicht zentral durch die Universität Siegen bereitgestellten bzw. lizensierten Meeting-Systemen und Cloud-Diensten ist zur Erhebung, Verarbeitung und Speicherung dienstlicher Daten nicht gestattet.

Folgende Ausnahmen gestatten die Nutzung anderer Dienste, entsprechend der jeweiligen Geschäftsbedingungen und unter Beachtung der Vorgaben in dieser Richtlinie:

[1]siehe IT-Grundschutzmaßnahmen zur IT-Sicherheit (IT-Anwender) der Universität Siegen vom 14.05.2014, https://www.uni-siegen.de/it-sicherheit/richtlinien/downloads/it-grundschutzkatalog_anwender.pdf

- **Nutzung von Diensten/Systemen unter der Federführung einer anderen Einrichtung**
- **Nutzung von Diensten/Systemen nach vorheriger Abstimmung mit der oder dem Datenschutzbeauftragten und der oder dem Informationssicherheitsbeauftragten zu datenschutzrechtlichen Belangen und notwendigen Sicherheitsmaßnahmen (Verzeichnis der Verarbeitungstätigkeiten und ggf. Auftragsverarbeitungsverträge, Erläuterungen zu technischen und organisatorischen Maßnahmen, Rollen- und Berechtigungskonzepte etc.)**

Grundsätzlich gilt, dass die Verbreitung sowie das Abrufen, Hochladen und die Bereitstellung von rechtswidrigen bzw. rechtswidrig erlangten Inhalten untersagt ist. Insbesondere Inhalte, die gegen datenschutzrechtliche, strafrechtliche, persönlichkeitsrechtliche, lizenzrechtliche oder urheberrechtliche Regelungen oder Bestimmungen verstoßen, sind nicht zulässig.

3.2 Datenkategorien

Auch bei der Nutzung von zentral bereitgestellten Meeting-Systemen und Cloud-Diensten dürfen nicht alle Datenkategorien verarbeitet und gespeichert werden. Bei Datenkategorien mit hohem (z.B. vertrauliche Daten, sensible personenbezogene Daten) müssen weitere Schutzmaßnahmen ergriffen werden. Daten mit einem sehr hohen Schutzbedarf dürfen nicht verarbeitet werden (siehe 6. Schutzbedarf).

Falls eine Verschlüsselung der Daten notwendig ist, muss die Verschlüsselung der Daten vor der Übertragung sichergestellt werden. Zur Verschlüsselung der Daten ist darauf zu achten, dass die genutzte Technik als sicher anerkannt ist und die vollständige Kontrolle bei den Nutzerinnen und Nutzern oder kompetenten Stellen an der Universität Siegen liegt.

3.3 Zugriffsberechtigungen

Vor der Übertragung von Daten an zentral bereitgestellte Meeting-Systeme und Cloud-Dienste müssen die Zugriffsberechtigungen und das Speicherziel geprüft werden. Die Vergabe von Berechtigungen an nicht zugriffsberechtigte Personen muss vermieden werden.

3.4 Löschung von Daten

Daten die beispielsweise einer gesetzlichen Löschverpflichtung unterliegen, sind für die Speicherung im Rahmen eines Cloud-Dienstes weniger geeignet. Es kann nicht ausgeschlossen werden, dass die Daten zwar in der Ansicht der Anwenderin oder des Anwenders als gelöscht erscheinen, jedoch tatsächlich (vorerst) nicht gelöscht werden. Gründe dafür könnten u.a. spezielle Speichertechniken sein, die eine Löschung der Daten erst nach einem gewissen Zeitraum zulassen.

3.5 Sparsamer Umgang mit Daten

Bei der Nutzung von Meeting-Systemen und Cloud-Diensten müssen die Datenmengen so gering wie nötig gehalten werden. Insbesondere gilt dies für die Verarbeitung von personenbezogenen und weiteren sensiblen Daten.

Primäre Speicherorte sind weiterhin die lokalen IT-Systeme der Universität Siegen wie Netzwerklaufwerke etc.

Bei der Übertragung größerer Datenmengen oder kompletter Verzeichnisstrukturen könnten leicht sensible Daten übersehen und versehentlich mit an den Clouddienst übertragen werden, was zu vermeiden gilt.

3.6 Dienstrechtliche Vorgaben

Für bestimmte Datenkategorien gelten ggf. dienstrechtliche Vorgaben, die eine Speicherung der Daten außerhalb von Speichersystemen der Universität Siegen untersagen. Diese Vorgaben sind zu beachten und bei eventueller Unklarheit bezüglich des Vorgehens ist die oder der jeweilige Dienstvorgesetzte mit einzubeziehen.

3.7 Backups von extern gespeicherten Daten

Nicht alle Anbieter verfügen über eine zusätzliche Backup-Option der in ihren Systemen gespeicherten Daten, weshalb es in diesen Fällen wichtig ist, dass jede Nutzerin und jeder Nutzer eigenständig für ein Backup der extern gespeicherten Daten auf dienstlichen Geräten und Systemen sorgt.

Für Backups von kompletten Clientsystemen sind die zentral bereitgestellten Backup-Systeme und -Dienste des ZIMTs zu verwenden.

3.8 Technische Voraussetzungen und Ausschlusskriterien

- Das Endgerät auf dem die Clientsoftware eingesetzt wird, muss den Vorgaben des IT-Grundschutzkatalogs für Anwender entsprechen.
- Insbesondere sind die Clientsoftware und die Software der Meeting-Systeme und Cloud-Dienste, auf dem neusten Stand zu halten. Sicherheitsupdates müssen umgehend installiert werden. Ein aktueller Virenscanner sowie eine aktive Firewall müssen vorhanden sein.
- Passwörter, die bereits bei Diensten der Universität Siegen genutzt werden, dürfen nicht für die Anmeldung an anderen Systemen verwendet werden.

Meeting-Systeme und Cloud-Dienste dürfen nicht von Systemen genutzt werden, die eine Server-Funktion haben, eine technische Anlage steuern oder die aus betrieblichen Gründen nicht den Anforderungen des IT-Grundschutzkatalogs für Anwender[1] genügen.

3.9 Vorgaben, Funktionen und Einstellungen zur Erhöhung der Informationssicherheit und des Datenschutzes

Funktionen und Einstellungen in Cloud-Diensten und Meeting-Systemen, die der Erhöhung der Informationssicherheit und des Datenschutzes dienen, sind, wenn technisch möglich, zu nutzen.

Von einer (ggf. automatisierten) Speicherung von Informationen in externen Cloud-Speichern im Zusammenhang mit Anwendungssoftware wie beispielsweise Office- oder Grafik-Software, ist, auch wenn bereits voreingestellt, abzusehen. Die entsprechenden Funktionen sind zu deaktivieren.

4. Besondere Regelungen für die Durchführung von Online-Meetings

Die Universität Siegen gibt besondere Regelungen für die Durchführung von Online-Meetings vor, die in der Handreichung zur Richtlinie zur Nutzung von Meeting-Systemen und Cloud-Diensten spezifiziert und regelmäßig aktualisiert werden.

Die in der Handreichung genannten Regelungen sind verbindliche Handlungsanweisungen.

5. Exportkontrollrechtliche Belange

Es sind exportkontrollrechtliche Belange für die Nutzung von Meeting-Systemen und Cloud-Diensten zu beachten, die im Rahmen der Handreichung zur Richtlinie zur Nutzung von Meeting-Systemen und Cloud-Diensten erläutert werden.

Die in der Handreichung genannten Regelungen sind verbindliche Handlungsanweisungen.

6. Schutzbedarf

Die Möglichkeit der Erhebung, Verarbeitung und Speicherung von Daten mit Hilfe der zentral bereitgestellten Meeting-Systeme und Cloud-Dienste hängt vom Schutzbedarf der Daten ab.

Der Schutzbedarf ist anhand einer Schutzbedarfsfeststellung[2] hinsichtlich der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit, vor einer Verarbeitung oder Speicherung der Informationen zu ermit-

[2] https://www.uni-siegen.de/it-sicherheit/richtlinien/downloads/it-grundschutzkatalog_anwender.pdf, siehe 9ff.

teln. Je nach Schutzbedarf müssen entsprechende Maßnahmen zur Einhaltung der Schutzziele getroffen werden (z.B. Verschlüsselung), ggf. ist eine Nutzung von Meeting-Systemen und Cloud-Diensten nicht zulässig.

Die Erhebung, Speicherung und Verarbeitung von personenbezogenen Daten unterliegen den Bestimmungen des Datenschutzes. Auch Daten ohne Personenbezug können, z.B. auf Grund von Geheimhaltungsvorschriften, einen hohen oder sehr hohen Schutzbedarf haben.

Grundsätzlich sind die Verwendung von Verschlüsselungsmechanismen und Verfahren zur Integritätssicherung empfehlenswert.

Der Schutzbedarf der Daten legt fest, ob eine Speicherung und Verarbeitung mit den zentral bereitgestellten Meeting-Systemen und Cloud-Diensten zulässig ist:

Schutzbedarf	Nutzung der zentral bereitgestellten Meeting-Systeme und Cloud-Dienste
Normal	Zulässig Verschlüsselung/Integritätssicherung empfohlen
Hoch	Nur mit vollständiger Verschlüsselung und Integritätssicherung zulässig
Sehr hoch	Nicht zulässig

Insbesondere sensible personenbezogene Daten sind nicht geeignet.

Beispiele für Daten, die entsprechend ihres Schutzbedarfes in den zentral bereitgestellten Meeting-Systemen und Cloud-Diensten verarbeitet werden können, werden in der Handreichung zur Richtlinie zur Nutzung von Meeting-Systemen und Cloud-Diensten aufgezeigt.

7. Hinweise zum Datenschutz

Auch bei der Nutzung von Meeting-Systemen und Cloud-Diensten gelten zur Verarbeitung von personenbezogenen Daten die allgemeinen gesetzlichen Bestimmungen. Diese sind derzeit für die öffentlichen Stellen des Landes das Datenschutzgesetz NRW (DSG NRW) und die EU-DSGVO.

Es ist hier insbesondere darauf zu achten, dass Dritte, die Zugriff auf personenbezogene Daten nehmen (könnten), sich zur Einhaltung dieser Regelungen verpflichten und entsprechende hinreichende Garantien für die gesetzeskonforme Verarbeitung erbringen müssen.

Für Dritte, die ihren Sitz in der EU haben, für deren Land ein Angemessenheitsbeschluss existiert (beispielsweise Japan, Schweiz, etc.) und für solche Unternehmen, die durch ein anderes von der EU-Kommission akzeptiertes Zertifizierungsverfahren (beispielsweise Privacy Shield, USA) zertifiziert sind, kann dies mittels einer obligatorischen Auftragsverarbeitungsvereinbarung (AVV) geregelt werden.

Für Dritte in anderen Nicht-EU-Ländern muss dies in jedem Einzelfall betrachtet werden.

Darüber hinaus muss für das Verfahren, in dem diese Systeme eingesetzt werden, eine Dokumentation mittels der Übersicht über Verarbeitungstätigkeiten (VVT) erstellt werden. Darin sind die genutzten Meeting-Systeme und Cloud-Dienste anzugeben.

Soweit diese Maßnahmen der Aufgabenerfüllung dienen sind diese Verarbeitungen in der Regel über Artikel 6 Absatz 1 e) DSGVO zulässig. Es ist daher auf die Erfüllung der Informationspflichten nach Artikel 13 DSGVO zu achten.

Sollte für die jeweilige Verarbeitung ausnahmsweise eine Einwilligung der betroffenen Personen gemäß Artikel 6 Absatz 1 a) DSGVO notwendig sein, ist diese im Vorfeld der Nutzung von den betroffenen Personen einzuholen. Es wird empfohlen, dieses Vorgehen mit der oder dem Datenschutzbeauftragten der Universität Siegen abzusprechen.

8. Einstellung der Nutzung von Meeting-Systemen und Cloud-Diensten

Die IT unterliegt dem ständigen technischen Wandel, weshalb Verfahren, die heute als sicher und nutzbar angesehen werden, sich zu einem späteren Zeitpunkt als nicht mehr ausreichend sicher herausstellen. Zudem können Sicherheitslücken entstehen die, die Sicherheit der Systeme bedrohen.

Es ist daher wichtig, sich vor dem Einsatz von Hard- und Software, insbesondere vor dem Einsatz von Meeting-Systemen und Cloud-Diensten regelmäßig über den Stand der Technik zu Sicherheitslücken oder ähnliches zu informieren. Bei drohendem Verlust von Vertraulichkeit, Integrität, Verfügbarkeit, die ebenfalls relevant für die Umsetzung datenschutzrechtlicher Belange der EU-DSGVO und des DSG-NRW sind, ist die Nutzung eines Dienstes einzuschränken oder einzustellen.

9. Veröffentlichung und Inkrafttreten

Diese Richtlinie wird in den Amtlichen Mitteilungen der Universität Siegen veröffentlicht. Sie tritt am Tag nach der Veröffentlichung in Kraft.

Ausgefertigt aufgrund des Beschlusses des Rektorats vom 2. Juli 2020.

Siegen, den 16. Juli 2020

Der Rektor
in Vertretung

gez.

(Universitätsprofessor Dr. Thomas Mannel)