Amtliche Mitteilung Nr. 06/2023

Ergänzende Nutzungsbedingungen der Kollaborations- und Office-Lösung Microsoft Teams für die Nutzung und Verarbeitung dienstlicher Daten

Herausgegeben am 31. Januar 2023

Technology
Arts Sciences
TH Köln

Ergänzende Nutzungsbedingungen der Kollaborations- und Office-Lösung Microsoft Teams für die Nutzung und Verarbeitung dienstlicher Daten

Aufgrund des § 2 Absatz 2 der Benutzungsordnung für die zentralen IT-Services der Campus IT hat die Campus IT der Technischen Hochschule Köln (im Folgenden „TH Köln“) die folgenden ergänzenden Nutzungsbedingungen zur Nutzung und Verarbeitung von dienstlichen Daten in der cloudbasierten Kollaborationslösung „Microsoft 365 Teams“ (im Folgenden „MS Teams“) erlassen:

Präambel

Diese Nutzungsbedingungen ergänzen und konkretisieren die grundsätzlichen Regelungen der Microsoft Service-Vereinbarungen, der Microsoft-Datenschutzbestimmungen und der Microsoft-Datenschutznachträge zwischen Microsoft (im Folgenden „Anbieterin“) und dem/der Endnutzer*in.

Sie beziehen sich auf die dienstliche Nutzung von MS Teams zu Zwecken von Forschung, Lehre und Hochschulverwaltung durch Mitglieder der Technischen Hochschule Köln. Diese Nutzungsbedingungen finden auf private Daten der Endnutzer*in keine Anwendung.

Wenn Daten mit Hilfe von weltweit jederzeit verfügbaren cloudbasierten Diensten an dynamisch verteilten Orten gespeichert bzw. verarbeitet werden, drohen besondere Gefahren. Diesen Risiken ist mit einer spezifischen Vorsorge hinsichtlich der Informationssicherheit und des Schutzes personenbezogener Daten zu begegnen.

Für die Speicherung und Verarbeitung von personenbezogenen Daten gilt insbesondere die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, nachfolgend „DSGVO“), das Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) und ggf. weitere nationale datenschutzrechtliche Regelungen (insbesondere das BDSG).

Die Endnutzer*innen der TH Köln sind für die bestimmungsgemäße Nutzung von MS Teams und der Einhaltung der Regelungen sowie für die sorgfältige Trennung zwischen privaten und dienstlichen Daten selbst verantwortlich.

Für private Daten der Endnutzer*innen gilt alleine der (End-)Nutzungsvertrag zwischen der Anbieterin und dem/der Endnutzer*in. Die Anbieterin ist diesbezüglich alleinige Verantwortliche im Sinne des Art. 4 S. 1 Nr. 7 DSGVO.

Für dienstliche, personenbezogene Daten der Endnutzer*innen der TH Köln, die im Rahmen ihrer dienstlichen Tätigkeit durch die Anbieterin verarbeitet werden sollen, gelten diese ergänzenden Nutzungsbedingungen. In Bezug auf die dienstlichen, personenbezogenen Daten gilt die TH Köln als Verantwortliche im Sinne des Art. 4 S.1 Nr. 7 DSGVO. Die Verarbeitung von dienstlichen, personenbezogenen Daten erfolgt durch die Anbieterin nur auf Weisung und im Auftrag der TH Köln.

§ 1 Geltungsbereich

(1) Die TH Köln stellt den Endnutzer*innen MS Teams in einer für die TH Köln angepassten Konfiguration bereit. Diese Konfiguration wird in der Servicebeschreibung der Campus IT (https://intern.th-koeln.de/arbeitsplatz/office365-teams_8368.php) beschrieben. Mit dieser Konfiguration sind derzeit die Funktionsmerkmale Chat, Dateiablage und -freigabe, Kollaboration an Office-Dokumenten und Videokonferenzen möglich. Das vorliegende Dokument befasst sich vorrangig mit den kollaborativen und officebasierten Komponenten von MS Teams. Für die Nutzung von MS Teams als Videokonferenzwerkzeug sind die bereits bestehenden Nutzungsempfehlungen für Videokonferenzlösungen zu beachten.

(2) Diese Nutzungsbedingungen beinhalten ergänzend zu den Bestimmungen aus den MS Teams-Nutzungsverträgen zwischen Endnutzer*in und der Anbieterin grundsätzliche Nutzungsregelungen für alle Endnutzer*innen der TH Köln, wenn Sie in Ausübung der dienstlichen Tätigkeit für die TH Köln MS Teams zur Nutzung von dienstlichen, personenbezogenen Daten nutzen möchten, die durch die Anbieterin im Auftrag der TH Köln erhoben, gespeichert und verarbeiten werden.

§ 2 Abgrenzung und Begriffsdefinitionen

(1) „Personenbezogene Daten“ sind alle Informationen im Sinne des Art. 4 Nr. 1 DSGVO, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine natürliche Person wird als identifizierbar angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

(2) „Besondere Kategorien personenbezogener Daten“ im Sinne des Art. 9 Abs. 1 DSGVO sind besonders sensible personenbezogene Daten. Hierunter fallen:

- Daten, aus denen die rassische und ethnische Herkunft hervorgeht,
- Daten, aus denen politische Meinungen hervorgehen,
- Daten, aus denen religiöse oder weltanschauliche Überzeugungen hervorgehen,
- Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht,
- genetische Daten im Sinne des Art. 4 Nr. 13 DSGVO,
- biometrische Daten im Sinne des Art. 4 Nr. 14 DSGVO), die zur eindeutigen Identifizierung einer natürlichen Person verarbeitet werden,
- Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) und
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(3) „Sachbezogene Daten“ sind Daten ohne Personenbezug im Sinne des Absatzes 1. Diese Daten können auch einen hohen Schutzbedarf haben, insbesondere wenn Sie ein Dienst- oder Geschäftsgeheimnis darstellen oder einer Vertraulichkeits- oder Geheimhaltungsvereinbarung unterliegen.

(4) „Dienstliche personenbezogene Daten“ sind personenbezogene Daten im Sinne des Absatzes 1, die durch den/die Endnutzer*in in Ausübung einer dienstlichen Tätigkeit zu Zwecken der Lehre, Forschung und Hochschulverwaltung in MS Teams eingebracht und verarbeitet werden.

§ 3 Schutzbedarf

(1) Für die Entscheidung, unter welchen Bedingungen eine Nutzung und Verarbeitung von dienstlichen, personenbezogenen Daten in MS Teams in Frage kommt, bildet der Schutzbedarf der dienstlichen, personenbezogenen Daten die grundlegende Richtschnur. Hinweise auf den Schutzbedarf können zum einen aus der systematisch durchgeführten Schutzbedarfsanalyse und zum anderen aus der Datenkategorie abgeleitet werden.

(2) Daten lassen sich in die folgenden Datenkategorien einteilen:

Datenkategorie	Hinweis auf typischen Schutzbedarf
Daten, die aus öffentlich zugänglichen und offenkundig legal zugänglichen Quellen stammen (z.B. Literatur und Dokumente)	Keinen
Sachbezogene Daten, die keine personenbezogenen Daten beinhalten	Keinen bis sehr hoch
Dienstliche (nicht wissenschaftliche) Daten	Normal bis sehr hoch
Dienstliche (nicht wissenschaftliche) Daten, z.B. Lehrveranstaltungsdaten (Teilnehmendenlisten)	Normal
Dienstliche (nicht wissenschaftliche) Daten, z.B. Fotos und Videos von öffentlichen Veranstaltungen ohne dass hierdurch Einzelpersonen oder kleine Gruppen hervorgehoben werden	Normal
Dienstliche (nicht wissenschaftliche) Daten, z.B. Prüfungsdaten (Prüfungsergebnisse, Notenlisten, Gutachten)	Hoch
Handgeschriebene Texte mit personenbezogenen Daten (z.B. Vor- und Nachname, Matrikelnummer etc.)	Hoch
Dienstliche (nicht wissenschaftliche) Daten, z.B. Video- und Audioaufnahmen von Befragungen (abhängig von Inhalt)	Hoch bis sehr hoch

Wissenschaftliche Daten ohne Vertraulichkeits-Anforderungen	Normal
Wissenschaftliche Daten, z.B. Untersuchungsergebnisse, vertrauliche Forschungsdaten	Hoch bis sehr hoch
Besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO: Gesundheitsdaten, politische Meinungen, Daten über die sexuelle Orientierung, biometrische Identifikations- und Verifikationsdaten (wie DNA, Augenablichtung, Gesichtsgeometrie, Fingerabdrücke, Stimme) etc.	Sehr hoch
Personalaktendaten	Sehr hoch

Folgenden Aspekte sind zu beachten:

- Für personenbezogene Daten gelten die Bestimmungen des Datenschutzes.
- Auch Daten ohne Personenbezug (sachbezogene Daten) können einen sehr hohen Schutzbedarf haben (zum Beispiel auf Grund von Vertraulichkeits- oder Geheimhaltungsvereinbarungen).

(3) 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 zur Nutzung in MS Teams:

Schutzbedarf	*Eignung für die Verarbeitung in MS Teams*
Daten mit keinem oder normalen Schutzbedarf	Ja
Daten mit hohem oder sehr hohem Schutzbedarf	Nein

Empfehlungen

Bevor Daten in MS Teams verarbeitet werden, sollten die im vorangegangenen Abschnitt betrachteten Abhängigkeiten zwischen der Datenkategorie, dem Schutzbedarf der Daten und der Eignung beachtet werden.

Schutzbedarf der Daten bestimmt den Umfang der Cloud-Nutzung

Aus dem Schutzbedarf der für eine Nutzung und Verarbeitung vorgesehenen Daten folgt nicht nur, ob eine Nutzung und Verarbeitung zulässig sind, sondern auch unter welchen Bedingungen dies geschehen kann. Dabei ist der Schutzbedarf getrennt nach den drei Schutzzielen Verfügbarkeit, Integri-

tät und Vertraulichkeit zu betrachten. Näheres muss Gegenstand spezifischer Festlegungen derjenigen Person sein, die den Bereich der Datenverarbeitung verantwortet (z.B. die Projektleitung bei Projekten, Initiator*in eines Raums in MS Teams).

Verfügbarkeit

Da die auf MS Teams bearbeiteten Daten und Dokumente redundant auf verschiedenen Servern gesichert werden, ist Verfügbarkeit unter normalen Umständen kein hindernder Faktor, ein temporärer oder permanenter Ausfall oder Datenverlust ist dennoch nicht komplett auszuschließen. Die TH Köln haftet nicht für Schäden aus dem Verlust von Daten. Endnutzer*innen sind daher für die regelmäßigen Datensicherungen auf Datenspeichersystemen der TH Köln verantwortlich. Zur Sicherstellung der Verfügbarkeit der Daten und Dokumente sind Speichermöglichkeiten der TH Köln außerhalb von MS Teams (zum Beispiel Speicherung auf den zentralen Netzlaufwerken der TH Köln) zu nutzen.

Integrität

Die technische Sicherstellung der Datenintegrität erfolgt durch spezielle Speichersysteme der Anbieterin. 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 MS Teams eine größere Angriffsfläche als Dienste, die ausschließlich hochschulintern 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 die/der Nutzer*in selbst geeignete Maßnahmen zur Gewährleistung der Integrität ergreifen. Beispielsweise können lokale Backups auf Netzlaufwerken der TH Köln im Zweifelsfall mit online abgelegten Daten abgeglichen werden.

Vertraulichkeit

Die Nutzerdaten werden durch die Anbieterin nicht an Dritte, insbesondere nicht an andere Privatunternehmen, weitergegeben und nicht durch diese verarbeitet. MS Teams bietet jedoch eine größere Angriffsfläche als ein nur hochschulintern angebotener Dienst (z.B. nur intern erreichbare Netzlaufwerke der Campus IT). Im Falle von Sicherheitslücken in der verwendeten Systemsoftware oder kompromittierten Zugangsdaten könnten unberechtigte Personen an vertrauliche Daten gelangen.

Bei Daten mit hohen oder sehr hohen Anforderungen an die Vertraulichkeit (insbesondere bei sensiblen personenbezogenen Daten im Sinne des Art. 9 Abs. 1 DSGVO, Dienst- und Geschäftsgeheimnissen) ist von der Ablage in MS Teams abzusehen.

§ 4 Schutzbedarfsanalyse

(1) Allgemein soll mit den folgenden tabellarisch aufgeführten Schadenskategorien der Schutzbedarf der zu verarbeitenden Daten festgestellt werden. Der Fragenkatalog ist angelehnt an die Richtlinien zum IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Der Schutzbedarf definiert sich dabei ausschließlich aus den anzunehmenden Schäden, die entstehen, wenn die Daten nach einem auslösenden Ereignis (durch spezifische Bedrohungen wie Passwort-Kompromittierung, Ausfall eines Dienstes, Verlust von Daten, fehlerhafte Dateifreigaben für unberechtigte Dritte etc.) beeinträchtigt werden und so mindestens einer der Grundwerte der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit) verletzt wird. Dabei ergibt sich der Schutzbedarf aus den unmittelbaren Schäden und durch die möglichen Folgeschäden (z.B. Schadensersatzforderungen, Ausfallkosten, Lahmlegen des Hochschulbetriebs).

Eine quantitative Bewertung mit bezifferten Schadenshöhen wäre hier zu aufwändig 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 aufzustellen, 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
- Finanzielle Auswirkungen

Diese Themenbereiche werden betrachtet unter den Aspekten:

- Integrität und Vertraulichkeit der Daten sowie Verfügbarkeit der Daten und Dienste

(2) Näheres muss Gegenstand bereichsspezifischer Festlegungen sein.

§ 5 Schutzbedarfskategorien

(1) Schutzbedarfskategorie „Keine“

Schäden haben keine oder nur eine unwesentliche Beeinträchtigung der Person oder der Institution zur Folge.

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. Ein möglicher Missbrauch personenbezogener Daten hat keine nennenswerten Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der/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.

Beeinträchtigung der Aufgabenerfüllung	Es ist keine oder nur eine äußerst geringe Beeinträchtigung zu erwarten.

In Ausnahmefällen liegt die maximal tolerierbare Ausfallzeit bei bis zu zwei Tagen.

(2) Schutzbedarfskategorie „Normal“

Schäden haben Beeinträchtigungen der Institution zur Folge.

Verstoß gegen Gesetze und Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen. Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen.
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als tolerabel eingeschätzt werden. Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der/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.
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen bei bis zu 8 Stunden.

(3) Schutzbedarfskategorie „Hoch“

Bei einer hohen Schutzbedarfskategorie ist von der Nutzung von MS Teams abzusehen.

Im Schadenfall tritt Handlungsunfähigkeit wichtiger Bereiche der Institution ein; Schäden haben erhebliche Beeinträchtigungen der selbst oder betroffener Dritter zur Folge.

Verstoß gegen Gesetze und Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen. Vertragsverletzungen mit hohen Konventionalstrafen.

Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. 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 Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von einzelnen betroffenen Personen als nicht tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen bei bis zu 4 Stunden.

(4) Schutzbedarfskategorie „Sehr hoch“

Bei einer sehr hohen Schutzbedarfskategorie ist von der Nutzung von MS Teams abzusehen.

Der Schadenfall führt zum totalen Zusammenbruch der Institution oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche, oder es besteht Gefahr für Leib und Leben von Personen.

Verstoß gegen Gesetze (z.B. Geschäftsgeheimnisgesetz, vertrauliche Daten der Hochschule, Betriebsgeheimnis) und Vorschriften/Verträge, z.B. Geheimhaltungsvereinbarung, Vertraulichkeitsvereinbarung bei Projekten	Fundamentaler Verstoß gegen Vorschriften und Gesetze, Vertragsverletzungen, deren Haftungsschäden ruinös sind.
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. Ein möglicher Missbrauch personenbezogener Daten

	würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
Beeinträchtigung der persönlichen Unversehrtheit; Gefahr für Leib und Leben.	Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich.
Negative Außenwirkung	Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenzgefährdender Art, ist denkbar
Finanzielle Auswirkungen	Der finanzielle Schaden ist für die Institution existenzbedrohend.
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen unter einer Stunde

§ 6 Nutzungsberechtigung und Registrierung

(1) Nutzungsberechtigt sind alle Mitglieder und Angehörigen der Technischen Hochschule Köln.

(2) Die Campus IT der TH Köln stellt Ihnen, wenn Sie nutzungsberechtigt sind, einen Identity Provider (IdP) zur Verfügung.

Dieser dient der Authentifizierung und Autorisierung der Mitglieder der TH Köln gegenüber externen Dienstanbietern, sogenannten Service Providern (SPs), im Rahmen der Infrastruktur für Authentifizierung und Autorisierung des Vereins zur Förderung eines Deutschen Forschungsnetzes e.V. (DFN-AAI). Die Authentifizierungs- und Autorisierungs-Infrastruktur DFN-AAI wird vom DFN-Verein verwaltet. Er schafft das notwendige Vertrauensverhältnis sowie einen organisatorischen und technischen Rahmen für den Austausch von Benutzerinformationen zwischen den teilnehmenden Einrichtungen, zu denen auch die TH Köln gehört, und Drittanbietern (wie die Anbieterin) in der DFN-AAI.

(3) Um MS Teams zu nutzen, benötigen Sie eine gültige campus-ID der TH Köln und das zugehörige Passwort.

(4) Bei Registrierung ihrer Benutzerkennung bei der Anbieterin werden Ihre personenbezogenen Daten an den jeweiligen Dienstanbieter übertragen, verarbeitet und evtl. auch beim Service Provider gespeichert. Diese Daten beinhalten u.a. auch personenbezogene Daten, wie Ihren Vornamen, Nachnamen, die Einrichtung, Ihre dienstliche E-Mailadresse der TH Köln, Ihre campus-ID und Ihren Status (Studierende*r/Beschäftigte*r).

Weitere Informationen über die Verarbeitung Ihrer personenbezogenen Daten können Sie den Datenschutzinformationen der Anbieterin entnehmen.

Die TH Köln trägt dafür Sorge, dass nur diejenigen personenbezogenen Daten im Rahmen des DFN-AAI herausgegeben werden, die für den Service erforderlich sind.

Passwörter gelangen nicht zu den Service Providern. Die Überprüfung Ihrer campus-ID und des Passwortes erfolgt immer am Identity Provider der TH Köln. Die gesamte Kommunikation erfolgt dabei ausschließlich verschlüsselt. Die TH Köln übernimmt allerdings keine Verantwortung oder Garantie bzgl. der im Rahmen der DFN-AAI verfügbaren Dienste oder der datenschutzgerechten Nutzung durch den jeweiligen Dienstanbieter.

§ 7 Pflichten der Endnutzer*in

(1) Der/die Endnutzer*in sorgt eigenverantwortlich für die Einhaltung dieser Nutzungsbedingungen und insbesondere der datenschutzrechtlichen, persönlichkeitsrechtlichen, lizenzrechtlichen und urheberrechtlichen Bestimmungen. Eine Nutzung mit rechtswidrigen Inhalten ist unzulässig und bei der Nutzung dürfen keine Rechte (Urheber-, Persönlichkeitsrechte, Vertraulichkeitsvereinbarungen etc.) von Dritten verletzt werden.

(2) Der/die Endnutzer*in trägt dafür Sorge, dass private Daten von den dienstlichen Daten getrennt in unterschiedlichen und entsprechend gekennzeichneten Dateiordnern eingebracht, gespeichert und verarbeitet werden.

(3) Der/die Endnutzer*in ist für die regelmäßige Durchführung und Evaluierung dauerhafter Datensicherungsmaßnahmen gegen Datenverlust der dienstlichen (insbesondere personenbezogenen) Daten verantwortlich und trifft hierzu ggf. geeignete Maßnahmen.

Insbesondere ist sicherzustellen, dass regelmäßige Sicherungskopien von den in Teams gespeicherten Daten und Dokumenten erstellt werden und zugriffsgeschützt außerhalb von Teams gespeichert werden (z.B. zentrale Netzlaufwerke der TH Köln).

(4) Dienstliche, personenbezogene Daten, die in Teams gespeichert werden, sind nach Erreichen des Verarbeitungszweckes durch den/die Endnutzer*in zu löschen. Gesetzliche Aufbewahrungsfristen, die eine weitere Speicherung erfordern oder erlauben, sind zu beachten. Hierfür sind die von der TH Köln bereitgestellten Dateispeichersysteme zu nutzen. Der/die Endnutzer*in beachtet, dass nach Ende der Vertragslaufzeit oder bei Kündigung des (Endnutzer-) Nutzungsvertrags bzw. bei Auslauf der Nutzungsberechtigung eine Löschung der Daten erfolgt und trifft hierzu geeignete Vorkehrungen gegen Datenverlust (z.B. rechtzeitiger Download der Daten).

(5) Zuvor ggf. erteilte Dateifreigabeberechtigungen sind frühestmöglich zu widerrufen, sofern die Dateifreigaben nicht mehr erforderlich sind.

(6) Der/die Endnutzer*in ermittelt vor Auslagerung von dienstlichen, personenbezogenen Daten oder sachbezogenen Daten, die einen hohen Schutzbedarf haben, die Datenkategorie und führt eine Schutzbedarfsanalyse durch. Der hierdurch festgestellte Schutzbedarf legt die zusätzlich zu treffenden organisatorischen und technischen Maßnahmen (wie Datensicherung, Anonymisierung, Pseudonymisierung etc.) fest. Die Feststellung der Maßnahmen hat unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu erfolgen.

§ 8 Schlussbestimmungen

Ergänzend gelten die Bestimmungen der Benutzungsordnung für die zentralen IT-Services der Campus IT, abrufbar unter: https://www.th-koeln.de/hochschule/ordnungen-der-zentralen-einrichtungen_52256.php

TH Köln

Gustav-Heinemann-Ufer 54

50968 Köln

www.th-koeln.de

Technology
Arts Sciences
TH Köln