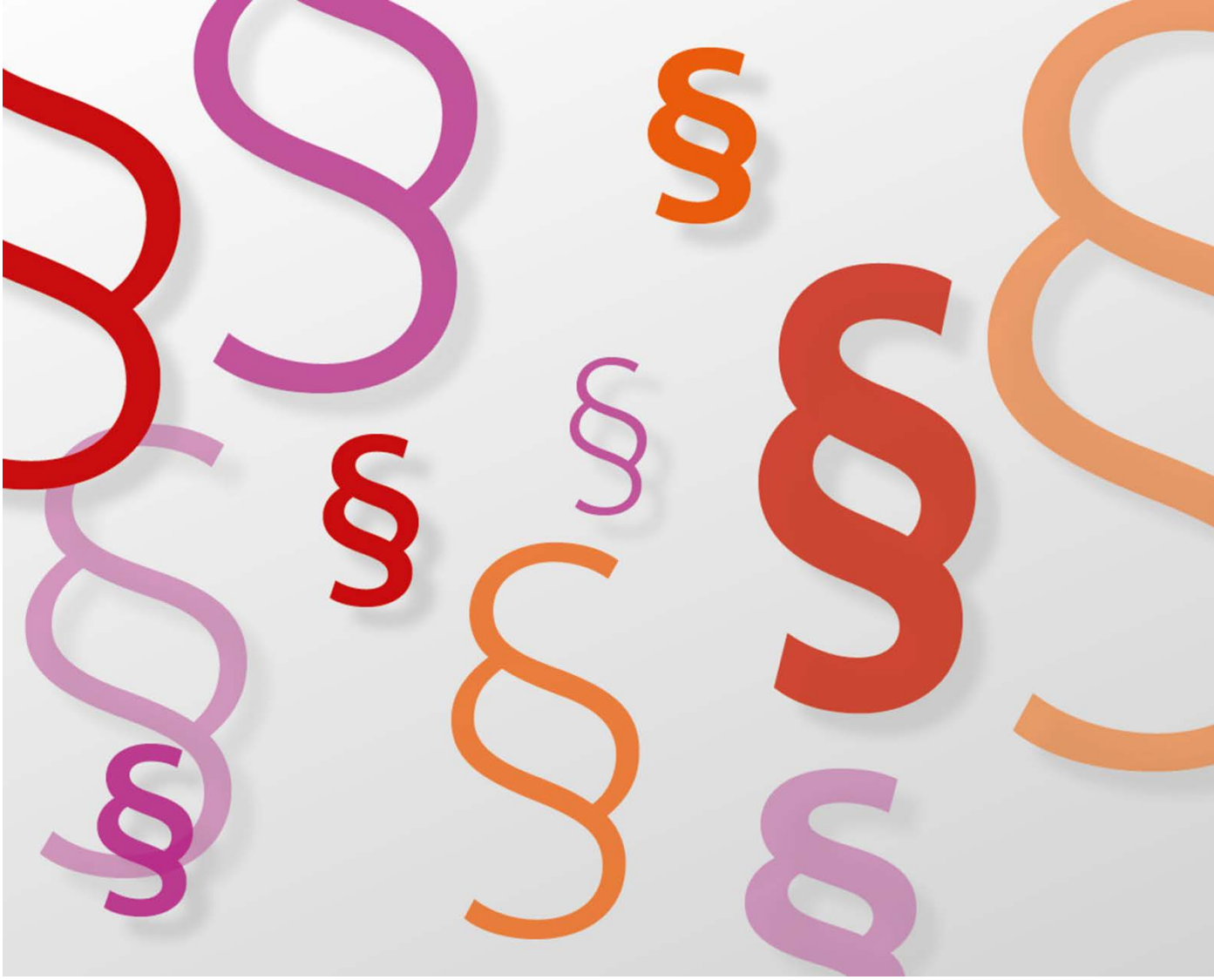

Amtliche Mitteilung Nr. 22/2019

Leitlinie zur Informationssicherheit und zum Datenschutz

Vom 7. November 2019

Herausgegeben am 15. November 2019

Technology
Arts Sciences
TH Köln

Hinweis:
Es wird darauf hingewiesen, dass gemäß § 12 Abs. 5 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz - HG NRW) eine Verletzung von Verfahrens- oder Formvorschriften des Ordnungs- oder des sonstigen autonomen Rechts der Hochschule nach Ablauf eines Jahres seit dieser Bekanntmachung nicht mehr geltend gemacht werden kann, es sei denn
1) die Ordnung ist nicht ordnungsgemäß bekannt gemacht worden,
2) das Präsidium hat den Beschluss des die Ordnung beschließenden Gremiums vorher beanstandet,
3) der Form- oder Verfahrensmangel ist gegenüber der Hochschule vorher gerügt und dabei die verletzte Rechtsvorschrift und die Tatsache bezeichnet worden, die den Mangel ergibt, oder
4) bei der öffentlichen Bekanntmachung der Ordnung ist auf die Rechtsfolge des Rügeausschlusses nicht hingewiesen worden.

Leitlinie zur Informationssicherheit und zum Datenschutz

Technology
Arts Sciences
TH Köln

Leitlinie zur Informationssicherheit und zum Datenschutz

Das Präsidium der Technischen Hochschule Köln (TH Köln) beschließt hiermit folgende Leitlinie zur Informationssicherheit und zum Datenschutz als Bestandteil ihrer Strategie:

Stellenwert der Informationsverarbeitung

Informationsverarbeitung spielt eine Schlüsselrolle für Forschung und Lehre. Alle wesentlichen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können. Der Schutz von Informationen aus Forschung und Lehre, von personenbezogenen Informationen aller Hochschulangehörigen und aller Informationen zum ordnungsgemäßen Betrieb der TH Köln vor unberechtigtem Zugriff und vor unerlaubter Änderung ist von existenzieller Bedeutung.

Übergreifende Ziele

Die Daten und IT-Services der TH Köln werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandszeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Services sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (Integrität). Die Anforderungen an Vertraulichkeit haben ein an Gesetzeskonformität orientiertes Niveau. Die Sicherheitsmaßnahmen müssen in einem vertretbaren Verhältnis zur Schutzklasse der Informationen und IT-Services stehen.

Alle Mitglieder und Angehörigen der TH Köln halten die einschlägigen Gesetze (z. B. Strafgesetzbuch, Sozialgesetzbuch, Gesetze und Regelungen zum Datenschutz, z. B. EU-DS-GVO) und vertraglichen Regelungen (z. B. zur Geheimhaltung) ein. Alle Hochschulmitglieder und -angehörigen und das Präsidium sind sich ihrer Verantwortung beim Umgang mit IT bewusst und unterstützen die Sicherheitsstrategie nach besten Kräften.

Detailziele

Die Datenschutzgesetze (DSG) und die Interessen der Mitglieder und Angehörigen der TH Köln verlangen eine Sicherstellung der Vertraulichkeit der personenbezogenen Daten (siehe auch DSG NRW). Die Daten und die IT-Services mit Bezug zu Personalservices und Student-Life-Cycle werden daher einem hohen Vertraulichkeitsschutz unterzogen.

Die Daten der Forschung und insbesondere der Drittmittel-Forschung haben sehr hohe (auch vertraglich geregelte) Vertraulichkeitsanforderungen. Durch deren Verlust oder Diebstahl können hohe Reputationsverluste entstehen. Durch technische und organisatorische Maßnahmen und die hohe Aufmerksamkeit der Hochschulmitglieder und -angehörigen wird die Vertraulichkeit geschützt und Manipulationen vorgebeugt.

Innerhalb des Campus-IT-Betriebes werden die Verfügbarkeit und die Fehlerfreiheit der Systeme sichergestellt. Stillstandzeiten sind nur in einem sehr geringen Maße akzeptabel, da diese direkt den Lehr- und Forschungsbetrieb stören können.

Die Nutzung des Internets zur Informationsbeschaffung und E-Mail zur Kommunikation ist für die TH Köln selbstverständlich. Durch entsprechende Maßnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

Datenschutz- und Informationssicherheitsmanagement

Zur Erreichung der Datenschutz- und Informationssicherheitsziele wurde in der TH Köln eine Sicherheitsorganisation (SKDI - Ständige Kommission Datenschutz und Informationssicherheit) eingerichtet. Es ist ein IT-

Sicherheitsbeauftragter (CISO – Chief Information Security Officer) benannt worden. Der CISO berichtet in seiner Funktion direkt an die SKDI. Die SKDI besteht aus der Vize-Präsidentin für Wirtschafts- und Personalverwaltung, den Datenschutzbeauftragten, dem Datenschutzmanager und dem CISO. Ständige Gäste in der SKDI sind jeweils ein/e Vertreter*in der beiden an der TH Köln aktiven Personalräte. Dem CISO und dem Campus-IT-Betrieb werden von der Hochschulleitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren und die durch die Hochschulleitung festgelegten Datenschutz- und Informationssicherheitsziele im Sinne dieser Leitlinie zu erreichen.

Der Campus-IT-Betrieb und der CISO sind durch die IT-Benutzer*innen ausreichend in ihrer Arbeit zu unterstützen.

Der CISO ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Sofern personenbezogene Daten betroffen sind, gilt gleiches für die Datenschutzbeauftragten.

Die IT-Benutzer*innen haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des CISO zu halten.

Es sind zwei Datenschutzbeauftragte bestellt. Den Datenschutzbeauftragten werden von der Hochschulleitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren und die durch die Hochschulleitung festgelegten Datenschutzziele im Sinne dieser Leitlinie zu erreichen.

Es ist ein Datenschutzmanager bestellt. Der Datenschutzmanager hat ein ausreichend bemessenes Zeitbudget für die Erfüllung seiner Pflichten zur Verfügung. Der Datenschutzmanager ist gehalten, sich regelmäßig weiterzubilden.

Sicherheitsmaßnahmen

Für alle Verfahren, Informationen, IT-Services wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen für bestimmte Rollen vergibt. Berechtigungen müssen ständig aktuell gehalten werden und bei Wegfall der Voraussetzungen gelöscht werden.

Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter*innen ihre Aufgaben erfüllen können.

Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt. Räume, in denen zentral hochschulweite IT-Services gehostet werden, werden zur Erreichung und Gewährleistung der Ziele dieser Leitlinie und zur Erhöhung der Arbeitssicherheit überwacht (Temperatur, Wassereinbruch, Stromausfall, Zutrittsprotokollierung, Videoüberwachung, etc.). Eine Leistungs- oder Verhaltenskontrolle der Beschäftigten hierbei findet nicht statt.

Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch geeignete Firewalls gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzer*innen durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen (SKDI, Datenschutzbeauftragte, Datenschutzmanager, CISO).

Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.

Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, muss auf Sicherheitsvorfälle zügig und konsequent reagiert werden. Maßnahmen für den Notfall werden in einem separaten Notfallvorsorgekonzept zusammengestellt. Ziel der TH Köln ist es, auch bei einem Systemausfall kritische Prozesse (Lehrbetrieb, Student-Life-Cycle, etc.) aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

Sofern IT-Services an externe Stellen ausgelagert werden, werden durch die Campus-IT konkrete Sicherheitsanforderungen in Service Level Agreements (SLA) vorgegeben. Das Recht auf Kontrolle wird festgelegt. Für umfangreiche oder komplexe Outsourcing-Vorhaben erstellt die Campus-IT ein detailliertes Sicherheitskonzept mit konkreten Maßnahmenvorgaben.

IT-Benutzer*innen nehmen regelmäßig an Schulungen zur korrekten Nutzung der IT-Services und den hiermit verbundenen Sicherheitsmaßnahmen teil. Die Hochschulleitung unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

Verbesserung der Informationssicherheit und des Datenschutzes

Das Managementsystem der TH Köln zur Informationssicherheit und zum Datenschutz wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Hochschulmitgliedern und -angehörigen bekannt sind, ob sie umsetzbar und in den Hochschulbetrieb integrierbar sind.

Die Hochschulleitung unterstützt die ständige Verbesserung des Sicherheits- und Datenschutzniveaus. Hochschulmitglieder und -angehörige sind gehalten, erkannte Schwachstellen und mögliche Verbesserungen an die entsprechenden Stellen (Vorgesetzte*r, Datenschutzbeauftragte*r, CISO) weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die IT-Sicherheit und den Schutz personenbezogener Daten weiter zu verbessern und ständig auf den aktuellen Stand zu halten.

Diese Leitlinie wird in den Amtlichen Mitteilungen der Technischen Hochschule Köln veröffentlicht und tritt am Tag nach ihrer Veröffentlichung in Kraft.

Ausgefertigt aufgrund des Beschlusses des Präsidiums vom 05.06.2019

Köln, den 07. November 2019

Der Präsident

der Technischen Hochschule Köln

Prof. Dr. Stefan Herzig

TH Köln
Gustav-Heinemann-Ufer 54
50968 Köln
www.th-koeln.de

Technology
Arts Sciences
TH Köln