Technische Universität München

Erheben Sie Studierendendaten?

Dann denken Sie an den Datenschutz!

Die TUM stellt für die Organisation des Studienbetriebs zentral das Campus-Management-System TUMonline und die E-Learning-Plattform Moodle bereit.

Weitere zentrale Angebote sind die Vorlesungsaufzeichnung, E-Mail- und Datenservices, Content-Management-Systeme, TUM Webformulare sowie kleinere Tools wie der TUManager zur Unterstützung der Prüfungsabwicklung.

Für Spezialfälle in der Lehre kann der ergänzende Einsatz von kommerzieller bzw. freier Software oder die Verwendung von Eigenentwicklungen sinnvoll sein. In all diesen Fällen sind etliche datenschutzrechtliche und sicherheitstechnische Aspekte zu beachten, da es sich bei Studierendendaten um personenbezogene Daten handelt. Personenbezogene Daten sind durch das bayerische Datenschutzgesetz besonders geschützt.

In dieser Broschüre erfahren Sie, was Sie bei der Erhebung, Speicherung und Verarbeitung von Studierendendaten datenschutzrechtlich und sicherheitstechnisch beachten müssen, wenn Sie eine die zentralen Dienste ergänzende Anwendung folgender Art einsetzen wollen:

- selbst beschaffte Software,
- Eigenentwicklungen,
- externe Webdienste zur Verarbeitung von Studierendendaten.

Inhalt

1. Welche allgemeinen Regeln der Datenverarbeitung sind zu beachten?

Ob Sie sich nun für den Einsatz eines externen Webdienstes, die Beschaffung und den Einsatz einer Software oder den Betrieb einer Eigenentwicklung zur Verwaltung von Studierendendaten entscheiden, einige wichtige Punkte müssen Sie immer beachten:

1.1 Verantwortung für die Datenverarbeitung

Die Gesamtverantwortung für den ordnungsgemäßen Umgang mit den Daten der Studierenden hat die Leitung der Einheit, an der der Dienst oder die Software eingesetzt wird. Entscheidet sich also ein Lehrstuhl für den Betrieb eines Systems, so ist die Lehrstuhlleitung in der Pflicht. Der Leitung müssen die eingesetzten Verfahren, das Risiko und die Sicherheitsmaßnahmen bekannt sein.

Jeder Beschäftigte ist allerdings auch persönlich zur Geheimhaltung und zum sorgfältigen Umgang mit personenbezogenen Daten verpflichtet.

1.2 Verfahrensfreigabe

Bei Anwendungen, in denen personenbezogene Daten gespeichert und verarbeitet werden, besteht die Pflicht, diese vom Datenschutzbeauftragten der TUM freigeben zu lassen. Hierfür ist eine Verfahrensbeschreibung einzureichen in der u. a. Zweck, Rechtsgrundlage, gespeicherte Daten und Löschfristen anzugeben sind.

Näheres unter
www.it.tum.de/studierendendaten
Stichwort: Verfahrensfreigabe

1.3 Besonderheiten bei Webanwendungen

Bei Webanwendungen, die öffentlich erreichbar sind, besteht die Pflicht, sowohl ein Impressum als auch eine Datenschutzerklärung auf den Webseiten zu veröffentlichen.

Näheres unter
www.it.tum.de/studierendendaten
Stichwort: Datenschutz beim Webauftritt

1.4 Datenpanne

Sollte es trotz aller Vorkehrungen passieren, dass Unbefugte Studierendendaten, die in Ihrer Verantwortung liegen, zur Kenntnis bekommen, so ist dies unverzüglich dem Datenschutzbeauftragten (sekretariat@datenschutz.tum.de) sowie dem TUM-Meldewesen zur IT-Sicherheit (it-sicherheit@tum.de) zu melden (Hochschulleitungsbeschluss vom 03.04.2012, siehe www.it.tum.de/studierendendaten Stichwort: Meldewesen).

2. Welche Probleme können bei der Nutzung externer Webdienste auftreten?

Es gibt viele Dienste zur Erhebung und Speicherung von Daten in der Cloud, sei es als Umfrage-Service, Online-Formular-Service oder auch Datenspeicher. Zumeist sind diese Dienste sehr intuitiv zu nutzen. Studierendendaten, z. B. die Anmeldung zu Lehrveranstaltungen, sind so schnell und unkompliziert erhoben. Der Einsatz solcher Tools ist aber mit einer Reihe von schwerwiegenden Problemen verbunden, die im Folgenden erläutert werden.

2.1 Datenschutz

Die Nutzung dieser kleinen Online-Helferlein ist mit der Bezahlung in einer meistens nicht auffälligen Währung verknüpft: mit Daten – hier mit den Daten unserer Studierenden.

Mitglieder der TUM sind gesetzlich dazu verpflichtet, Studierendendaten zu schützen. Deshalb dürfen sie diese – unabhängig vom Geschäftsmodell des Anbieters – nicht einfach aus der Hand geben. Daten dürfen nicht ohne weiteres an einen externen Dienst weitergegeben werden.

Ebenso dürfen die Studierenden nicht ohne Weiteres verpflichtet werden, Daten dort selbst zu erfassen.

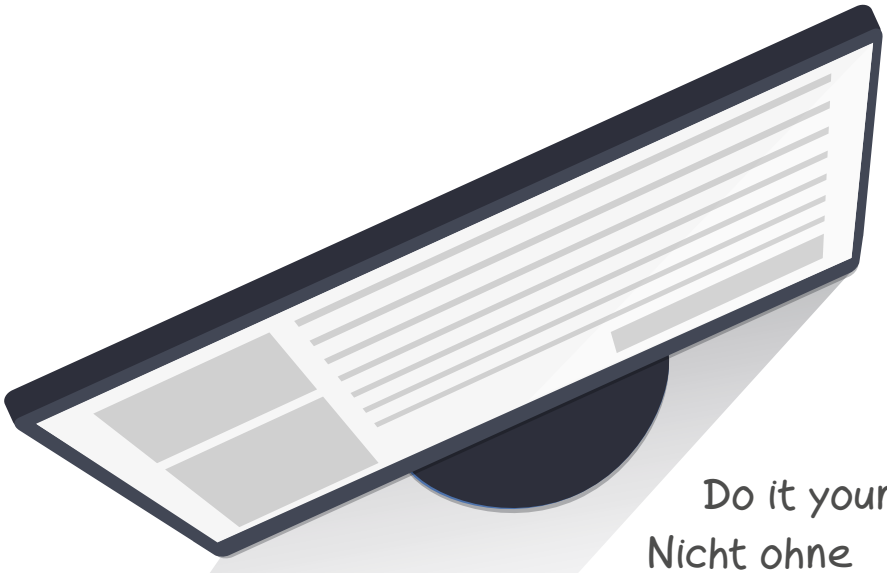
Dieser Weg ist nur unter der Voraussetzung möglich, dass der Anbieter über eine sogenannte Auftragsdatenverarbeitung per Vertrag an die Einhaltung aller datenschutzrechtlich relevanten Aspekte gebunden wird.
Näheres unter
www.it.tum.de/studierendendaten
Stichwort: externe Verarbeitung

Es ist davon auszugehen, dass bei Diensten wie Google-Forms eine derartige vertragliche Bindung nicht möglich ist. Dieser Dienst darf damit für die Erhebung von Studierendendaten (auch auf freiwilliger Basis) nicht verwendet werden!

2.2 IT-Sicherheit

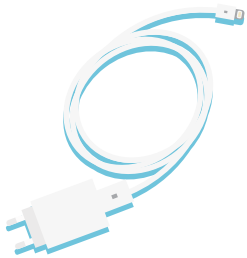
Haben Sie einen Anbieter gefunden, der Ihre Anforderungen erfüllt und der bereit ist, einen Vertrag über Auftragsdatenverarbeitung abzuschließen, müssen Sie sich versichern, dass der Anbieter sich auch um die Sicherheit der Daten kümmert. Gute Anzeichen hierfür sind Zertifikate zur IT-Sicherheit oder Datenschutzgütesiegel.

Eine Übersicht von Datenschutzgütesiegeln bietet die Stiftung Datenschutz. Näheres unter
www.it.tum.de/studierendendaten
Stichwort: Gütesiegel

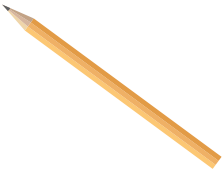


Do it yourself?
Nicht ohne

- ☑ verantwortliche Person für Updates und Wartungsarbeiten
- ☑ ausreichende Qualitätssicherung
- ☑ IT-Sicherheitskonzept
- ☑ regelmäßige Sicherheitsupdates



3. Auf was ist bei Kaufsoftware, freier Software und Eigenentwicklungen zu achten?



3.1 Qualität wichtiger als Preis

Ob Sie nun bereits existierende Software beschaffen oder diese selbst entwickeln oder entwickeln lassen: Bei der Auswahl der Software, der Firma oder Person, die für Sie entwickeln soll, ist es wichtig, Qualität und Professionalität über den Preis zu stellen.

Software, für die es regelmäßig Sicherheitsupdates gibt, und Entwickler mit ausreichender Erfahrung sorgen eher für ein ausreichendes Sicherheitsniveau, das für Studierendendaten benötigt wird, als nebenbei „kurz mal“ programmierte Schnellschüsse.

So verringern Sie bereits im Vorfeld die Gefahr von Datenpannen. An ein IT-Sicherheitskonzept sollte bereits in der Planungsphase gedacht werden, um so sicherzustellen, dass diese wichtigen Punkte bereits in der Entwicklung mit einfließen.

Zudem ist sicher zu stellen, dass die Anwendung betreut wird, solange sie in Betrieb ist. Hier muss langfristig eine verantwortliche Person für Updates und sonstige Wartungsarbeiten benannt sein. **Ohne verantwortliche Person ist die Anwendung vom Netz zu nehmen.**

4. Ort der Datenspeicherung

Ein wesentlicher Punkt für den Datenschutz ist der Ort, an dem Sie die personenbezogenen Daten der Studierenden ablegen.

4.1 Extern

Werden die Daten auf einem externen Server, also außerhalb des Münchner Wissenschaftsnetzes (MWN), gespeichert, so ist der Anbieter, der den Server betreibt, über eine Auftragsdatenverarbeitung (ADV) per Vertrag an die Einhaltung aller datenschutzrechtlich relevanten Aspekte zu binden.
Dies geht nur mit Anbietern innerhalb der EU / des Europäischer Wirtschaftsraum (EWR) und in einigen sogenannten sicheren Drittländern.

In diesen Fällen müssen Sie sich nicht selbst um die Sicherheit der Systeme kümmern. Allerdings sind Sie verpflichtet, sich über die Sicherheitsmaßnahmen zu informieren und diese zu überprüfen.
Näheres zur Auftragsdatenverarbeitung unter www.it.tum.de/studierendendaten
Stichwort: Externe Verarbeitung

4.2 Leibniz-Rechenzentrum (LRZ)

Das LRZ bietet als Rechenzentrum der TU München, LMU und Bayerischen Akademie der Wissenschaften das Hosting virtueller Server an und übernimmt dort bereits viele sichernde Maßnahmen. Die für die Speicherung von Studierendendaten notwendigen vertraglichen Regelungen zur ADV sind zwischen TUM und LRZ bereits in einem Rahmenvertrag getroffen. Das LRZ gilt damit aus der Sicht des Datenschutzes als interne Stelle. Damit ist das LRZ sowohl durch die vertragliche Bindung als auch durch den professionellen Rechenzentrumsbetrieb eine sehr gute Wahl. Informieren Sie sich, welche Leistungen das LRZ übernimmt und für welche Wartungsarbeiten Sie selbst zuständig sind. Das LRZ übernimmt üblicherweise nur die Wartung des Servers, nicht der Anwendung.
Näheres zum Serverbetrieb am LRZ unter www.it.tum.de/studierendendaten
Stichwort: Server am LRZ

4.3 Eigener Server

Natürlich können Sie auch einen eigenen Server im Netz der TUM betreiben und dort die Daten der Studierenden speichern. Für Server und Anwendung ist dann eine kontinuierliche Betreuung sicher zu stellen, um regelmäßig Sicherheitsupdates einzuspielen und neueste Angriffe umgehend abwehren zu können.
Näheres unter
www.it.tum.de/studierendendaten
Stichwort: Eigener Server

5. Auf welche Besonderheiten ist bei Webanwendungen zu achten?

Neben der bereits erwähnten Pflicht, ein Impressum und eine Datenschutzerklärung auf der Webseite zur Verfügung zu stellen, gibt es einige wichtige Punkte bezüglich der IT-Sicherheit, die beachtet werden sollten. Webanwendungen sind durch die öffentliche Erreichbarkeit im Internet besonders angreifbar. Deshalb empfehlen wir bei Eigenentwicklungen Sicherheitstests durch erfahrene Fachkräfte der IT-Sicherheit vor dem erstmaligen Einsatz.

Beachten Sie zudem Folgendes, wenn Sie Studierendendaten erheben oder verwalten:

- Die Webanwendung darf nur verschlüsselte Verbindungen zulassen, d. h. sie darf ausschließlich über https://… erreichbar sein, wenn Sie personenbezogene Daten erheben.

- Die Nutzerdaten, die auf dem Webserver gespeichert werden, müssen so gut wie möglich vor unbefugtem Zugriff geschützt werden, z. B. durch Verschlüsselung der Daten, Zugriffskonzept, …

- Verwenden Sie für Ihre Webapplikation eine TUM-Domain. Das sorgt auch für Klarheit bei den Studierenden, wem Sie die Daten übergeben. Näheres unter www.it.tum.de/studierendendaten Stichwort: Webseiten

- Als Zertifikat für die verschlüsselte Verbindung verwenden Sie ein kostenloses DFN-Zertifikat. Näheres unter www.it.tum.de/studierendendaten Stichwort: Zertifikate

- Ihr eigener Webserver sollte sich physikalisch im Münchner Wissenschaftsnetz (MWN) befinden: www.it.tum.de/studierendendaten Stichwort: MWN
  Optimal ist die Nutzung eines Webservers am LRZ. Näheres unter www.it.tum.de/studierendendaten, Stichwort: Webserver am LRZ

6. Checkliste

Die TUM empfiehlt Ihnen die Nutzung der zentralen Systeme. Wie die nebenstehende Tabelle zeigt, werden hier die allgemeinen Pflichten zu Datenschutz und IT-Sicherheit zentral übernommen.

Die wichtigsten zentralen Systeme für Studierendendaten:

- ➔ TUMonline: zentrales Campus-Management-System
- ➔ Moodle: zentrale Lernplattform
- ➔ TUManager: zentrales Tool zur Prüfungsabwicklung

www.it.tum.de/studierendendaten
Stichwort: zentrale Systeme

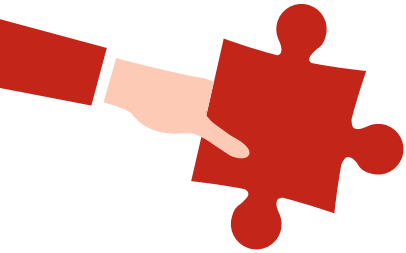
Einsatz von TUMonline Moodle, TUManager

Verantwortung für die Datenverarbeitung
☑ TUM

Maßnahmen Datenschutz
☑ Alle notwendigen Basismaßnahmen sind von der TUM getroffen

Maßnahmen IT-Sicherheit
☑ Alle notwendigen Basismaßnahmen sind von der TUM / dem LRZ getroffen

Auf den folgenden Seiten finden Sie kurze Checklisten, die Ihnen nochmal einen Überblick über Ihre Pflichten geben, falls Sie eigene Systeme bzw. Verfahren einsetzen.



Einsatz von eigenen Verfahren (z. B. Online-Anmeldung) auf Basis von Diensten der TUM, wie z. B. TUM Webformulare

Verantwortung für die Datenverarbeitung

Leitung der Einheit, die den Dienst/die Software einsetzt

☐ ggf. Beauftragten benennen

Maßnahmen Datenschutz

☐ Verfahrensfreigabe notwendig (siehe 1.2)?

➔ Wenn ja, Freigabe beim Datenschutzbeauftragten beantragen

Maßnahmen IT-Sicherheit

☐ Alle notwendigen Basismaßnahmen sind von der TUM/dem LRZ getroffen

Einsatz von eigenen Verfahren auf Basis von Diensten des LRZ, wie z. B. Nutzung virtueller Server mit selbst installierter (gekaufter/selbst entwickelter) Software

Verantwortung für die Datenverarbeitung

Leitung der Einheit, die den Dienst/die Software einsetzt

☐ ggf. Beauftragten benennen

Maßnahmen Datenschutz

☐ Verfahrensfreigabe notwendig (siehe 1.2)?

➔ Wenn ja, Freigabe beim Datenschutzbeauftragten beantragen

Maßnahmen IT-Sicherheit

Viele Maßnahmen sind vom LRZ getroffen, allerdings sind für die zusätzlich installierte Software weitere Maßnahmen zu ergreifen:

☐ IT-Sicherheitskonzept erstellen und umsetzen (siehe 3.1)

☐ Festlegung eines technisch Verantwortlichen, der sich langfristig und konsequent um die Wartung des Systems kümmert (siehe 3.1)

☐ Ist die Anwendung über das Web erreichbar?

➔ Wenn ja, Besonderheiten der Webanwendungen beachten (siehe 5)

Einsatz eines Verfahrens auf einem eigenen Server

Verantwortung für die Datenverarbeitung

Leitung der Einheit, die den Dienst/die Software einsetzt

☐ ggf. Beauftragten benennen

Maßnahmen Datenschutz

☐ Verfahrensfreigabe notwendig (siehe 1.2)?

➔ Wenn ja, Freigabe beim Datenschutzbeauftragten beantragen

Maßnahmen IT-Sicherheit

☐ IT-Sicherheitskonzept erstellen und umsetzen (siehe 3.1)

☐ Festlegung eines technisch Verantwortlichen, der sich langfristig und konsequent um die Wartung des Systems kümmert (siehe 3.1)

☐ Ist die Anwendung über das Web erreichbar?

➔ Wenn ja, Besonderheiten der Webanwendungen beachten (siehe 5)

Einsatz von externen Diensten

Verantwortung für die Datenverarbeitung

Leitung der Einheit, die den Dienst/die Software einsetzt

☐ ggf. Beauftragten benennen

Maßnahmen Datenschutz

☐ Verfahrensfreigabe notwendig (siehe 1.2)?

➔ Wenn ja, Freigabe beim Datenschutzbeauftragten beantragen

➔ Wenn ja, Abschluss eines Vertrags zur Auftragsdatenverarbeitung (siehe 2.1)

Maßnahmen IT-Sicherheit

☐ Prüfung der IT-Sicherheit des externen Anbieters (z. B. durch Vorlage des IT-Sicherheitskonzepts, Gütesiegel etc.; siehe 2.2)

☐ Ist die Anwendung über das Web erreichbar?

➔ Wenn ja, Besonderheiten der Webanwendungen beachten (siehe 5)

7. Fazit

Durch die Verpflichtung, mit Studierendendaten gesetzeskonform und damit besonders sorgfältig umzugehen, entstehen viele Aufgaben. Die Nutzung zentraler Dienste entlastet Lehrstühle oder andere Organisationseinheiten bei vielen dieser Aufgaben. Gerne hilft Ihnen der IT-Support bei der Suche nach dem richtigen Ansprechpartner für eine Umsetzung Ihrer Anforderungen mit einer TUM-internen Lösung.

Kontakt zum IT-Support

Der IT-Support hilft gerne bei der Suche nach dem richtigen Ansprechpartner zur Abbildung Ihrer Anforderung in TUM-interne Lösungen.

Kontaktieren Sie hierfür oder auch für sonstige Fragen zur IT:
it-support@tum.de

Fragen zum Datenschutz

Bei Fragen zum Datenschutz wenden Sie sich an:
sekretariat@datenschutz.tum.de

Herausgeber
Technische Universität München

Dipl.-Inf. Hans Pongratz
Geschäftsführender Vizepräsident für IT-Systeme und Dienstleistungen (CIO)
Arcisstr. 21, 80333 München
www.it.tum.de

Prof. Dr. Uwe Baumgarten
Datenschutzbeauftragter
www.datenschutz.tum.de