Technical University of Munich

Do you handle student data?

Then think about data protection!

To organize the university‘s degree programs, TUM offers the campus management system TUMonline and the e-learning platform Moodle.

Other centralized services include lecture recording, email and data services, content management systems, the TUM onlineforms and smaller tools, such as TUManager, for supporting the examination process.

In special cases, it can make sense to rely on additional commercially available software, freeware or proprietary programs for teaching activities. In these situations, it is important to adhere to all aspects of data protection and IT security given that handling student data involves personal information which is subject to special protection, as specified in the Bavarian Data Protection Act (BayDSG).

Grafik: iStock.com/
Künstler: macrovector

This booklet outlines what you have to consider with respect to data protection and IT security when collecting, storing and managing student data with one of the following types of applications as a supplement to the centralized services:

- Software you purchase independently,
- Software you develop independently (proprietary) ,
- External web services

Content

1. What general guidelines must be observed when managing student data?

Whether you elect to go with an external web service, the purchase and use of a software program or the use of proprietary programs for managing student data, there are several key points you must consider:

1.1 Responsibility for Data Management

The overall responsibility for properly handling student data lies with the head of the unit where the service or software is being utilized. If a TUM school or department decides to use a particular system for instance, the head of that unit bears responsibility. He/She must understand the associated processes and be aware of risks and required security measures.

However all employees are personally obligated to maintain confidentiality and use prudence when handling personal data.

1.2 Procedural Release

The TUM data protection official must approve applications in which personal data is stored and managed before use. This requires submitting a procedure description that includes the purpose, legal framework, the data to be stored and the deletion timeframes.

Additional information is available at
www.it.tum.de/en/studentdata/
Keyword: Procedural release

1.3 Web Applications

Publicly available web applications must have an imprint and a data protection statement on the website.

Additional information is available at
www.it.tum.de/en/studentdata/
Keyword: Data protection on websites

1.4 Data Breaches

If, despite all precautionary measures, unauthorized persons gain access to any student data for which you are responsible, immediately notify the TUM data protection official sekretariat@datenschutz.tum.de. Also, submit an incident report through the TUM IT security notification system it-sicherheit@tum.de (Decision made by the university's management team on April 3, 2012 concerning the establishment of a centralized security incident reporting system)
See www.it.tum.de/en/studentdata/
Keyword: IT security reporting

Designed by Freepik.com

2. What kind of issues can arise when using an external web service?

There are many cloud services to collect and save data, such as surveys, online forms or storage services. These services are very easy and intuitively to operate. In this way, student data, like a registration for courses, is collected quickly and easily. However, the use of such tools is tied to a wide range of serious issues as outlined below.

2.1 Data protection

The use of these small online aids is coupled with payment through a not-so-obvious currency: data - in this case, our student data. Members of TUM are obligated to protect student data. For this reason, you are not permitted to simply hand this information off to a third party, regardless of the provider‘s business model. Data may not be casually forwarded to an external provider. Likewise, students cannot be compelled to enter data on these systems themselves.

This approach is possible only under the condition that the provider is contractually bound to adhere to all relevant data protection regulations through a so-called contract data processing (CDP) agreement.

Additional information is available at
www.it.tum.de/en/studentdata/
Keyword: External providers

You can assume that this type of contractual commitment is not possible with services such as Google Forms. For this reason, this service may not be utilized for capturing student data (not on a voluntary basis either)!

Designed by Ibrandify/Freepik

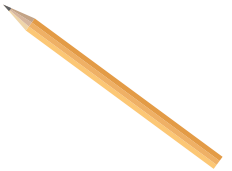
2.2 IT Security

If you have identified a provider that meets your requirements and is willing to sign an agreement for contract data processing, you must ensure that the data will be properly safeguarded. Good indicators include IT security certificates or data protection seals.
An overview of data protection seals is available through the independent Data Protection Foundation in Leipzig.

Additional information is available at
www.it.tum.de/en/studentdata/
Keyword: Seal of approval

Designed by Freepik.com

3. What should you consider when using purchased software, freeware or proprietary programs?



3.1 Quality More Important Than Price

Whether you acquire existing software, develop it on your own or have it developed by a third party: when selecting the software or the company or person to develop it for you it is important that you place quality and professionalism above price.

In contrast to hastily programmed, off-the-cuff solutions, software with regular security updates and developers with sufficient experience normally provides the level of security required for handling student data. This lets you reduce the risk of data breaches on the front end. Thought should be given to an IT security concept during the planning phase to make sure that this important issue is incorporated into the development process.

You must also ensure support for the application for as long as it is used. That means giving someone the long-term responsibility for updating and otherwise maintaining the software.

If no one has this responsibility, remove the application from the network.

4. Storage Location

A key issue with respect to data protection is where student personal data is stored.

Designed by Freepik.com

4.1 External

If the data is stored on an external server - meaning outside of the Munich Research Network (MWN) - the provider operating the server must be contractually bound to adhere to all relevant data protection regulations through a so-called contract data processing (CDP) agreement. This is possible only with providers in the European Union/European Economic Area and in so-called „secure third countries“. Although in these cases you are not responsible for actually managing the security of the systems, you are still obligated to understand and review the security measures implemented by the provider.

Additional information about contract data processing is available at
www.it.tum.de/en/studentdata/
Keyword: External Processing

4.2 Leibniz Supercomputing Center (LRZ)

In its role as the computing center for TUM, LMU and the Bavarian Academy of Science, the LRZ offers virtual server hosting and assumes responsibility for the corresponding security measures. The guidelines for storing student data as outlined in the CDP are already reflected in the framework agreement between TUM and LRZ. From the standpoint of data protection, the LRZ is thus viewed as an internal location. The contractual commitment plus the professional operation of the computing center makes LRZ an excellent choice for storing student data. Learn more about what services LRZ is responsible for and which maintenance activities are in your sphere of responsibility. LRZ typically assumes responsibility for server maintenance, not the application.
Additional information about LRZ server hosting is available at
www.it.tum.de/en/studentdata/
Keyword: Server at LRZ

4.3 Operating your own Server

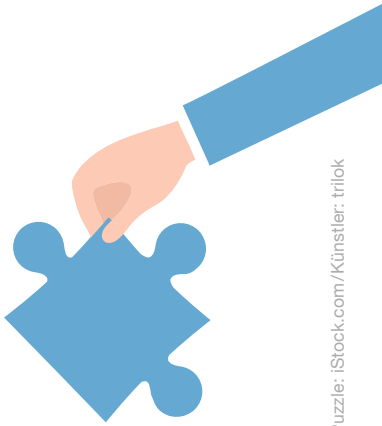
Of course, you can operate your own server on the TUM network and store student data on it. In this case, you must ensure that the server and application are supported on a continuing basis, to install the regular security updates and promptly fend off the latest hacker threats.
Additional information is available at
www.it.tum.de/en/studentdata/
Keyword: Own server

5. What do you have to consider when using web applications?

Apart from the aforementioned requirement to place an imprint and a data protection statement on the website, there are several important issues related to IT security you should keep in mind. Due to public availability through the Internet, web applications are particularly vulnerable to threats. For this reason, if you are using your own software, we recommend that an experienced IT security professional tests your system before bringing it online.

Furthermore, keep the following in mind when capturing or administering student data:

- If you are handling personal data, use only encrypted sessions for your web applications. That means they are only available via https://...
- User data stored on a web server must be provided maximum protection against unauthorized access, such as encrypting the data or creating an access rights concept
- Utilize a TUM domain for your web application. This provides clarity so that students know to whom they are giving their data.
  Additional information is available at
  www.it.tum.de/en/studentdata/
  Keyword: Website
- Use a DFN certificate (free of charge) for encrypted sessions.
  Additional information is available at
  www.it.tum.de/en/studentdata/
  Keyword: Certificates
- Your web server should physically belong to the Munich Research Network www.it.tum.de/en/studentdata/
  Keyword: MWN
  Ideally, you should use one of the LRZ web servers.
  Additional information is available at
  www.it.tum.de/en/studentdata/
  Keyword: Web server at LRZ



Hände mit Puzzle: iStock.com/Künstler: trilok

6. Checklists

TUM recommends the use of the central IT services. As shown in the table beside all general obligations concerning data protection and IT security are taken over by the service provider.

The most important IT systems hosting student data:

➔ TUMonline: central campus management system
➔ Moodle: central e-learning platform
➔ TUManager: central tool for supporting the examination process
www.it.tum.de/en/studentdata/
Keyword: Centralized it services

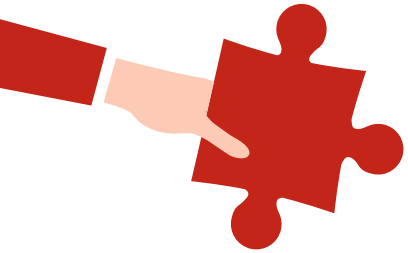
Utilizing TUMonline, Moodle, TUManager

Responsibility for handling data
☑ TUM

Data protection measures
☑ Required basic measures implemented by TUM

IT-Security measures
☑ Required basic measures implemented by TUM/LRZ

The following pages give you an overview of your obligations, in case you use your own systems or processes.



Utilizing an in-house process (i.e. online registration) with TUM services such as the TUM onlineforms

Responsibility for handing data
Head of the unit where the software is utilized
☐ If necessary, appoint representative

Data protection measures
☐ Procedural release required? (see 1.2)
➔ If yes, apply for approval for autonomed procedures at the data protection official

IT-Security measures
☐ Many measures are are implemented by TUM/LRZ

Utilizing an in-house process with LRZ services, such as a virtual server with self-installed software (purchased, self-developed)

Responsibility for handling data
Head of the unit where the software is utilized
☐ If necessary, appoint representative

Data protection measures
☐ Procedural release required? (see 1.2)
➔ If yes, apply for approval for autonomed procedures at the data protection official

IT-Security measures
Many measures are implemented by LRZ, however, further measures are necessary for self-installed software:
☐ Create and implement IT security concept (see 3.1)
☐ Appoint a responsible person who takes care of the long-term and consistent maintenance of the system (see 3.1)
☐ Is the application reachable via the web?
➔ If yes, consider special measures for web applications (see 5)

Utilizing a process on your own server

Responsibility for handling data
Head of the unit where the software is utilized
☐ If necessary, appoint representative

Data protection measures
☐ Procedural release required? (see 1.2)
➔ If yes, apply for approval for autonomed procedures at the data protection official

IT-Security measures
☐ Create and implement an IT security concept (see 3.1)
☐ Identify a person responsible for long-term, periodic maintenance of the system (see 3.1)
☐ Is the application reachable via the web?
➔ If yes, consider special measures for web applications (see 5)

Utilizing external service

Responsibility for handling data
Head of the unit where the software is utilized
☐ If necessary, appoint representative

Data protection measures
☐ Procedural release required? (see 1.2)
➔ If yes, apply for approval for autonomed procedures at the data protection official
➔ If yes, complete a contract data processing agreement (see 2.1)

IT-Security measures
☐ Check the IT security of the external provider (e.g. IT security concept, certificates or seals; see 2.2)
☐ Is the application reachable via the web? (siehe 3.1)
➔ If yes, consider special measures for web applications (see 5)

7. Summary

The obligation to prudently handle student data in compliance with the law involves a wealth of duties and responsibilities. By utilizing the university‘s centralized services, TUM schools, departments and other organizational units can relieve themselves of many of these responsibilities. IT-Support will gladly assist you in finding the right point of contact in order to implement your requirements for an internal TUM solution.

Contact the IT-Support

The IT-Support gladly likes to help you find the right partner to address your requirements on TUM solutions.

Therefore and for all other questions contact the IT-Support at
it-support@tum.de

Questions concerning data protection

For questions regarding data protection, please contact:
sekretariat@datenschutz.tum.de

Editor
Technical University of Munich

Dipl.-Inf. Hans Pongratz
Senior Vice President
Chief Information Officer (CIO)
Arcisstr. 21, 80333 München
www.it.tum.de

Prof. Dr. Uwe Baumgarten
Data Protection Offical
www.datenschutz.tum.de