GDPR

The focus of this part will be on the key concepts of the General Data Protection Regulations, also known as GDPR. The European Data Protection Regulation is applicable in all EU member states from 2018. It addresses the use of personal data in companies and organisations, such as universities.

Personal data

In the EU regulation, the concept of ***'personal data'*** *means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"* (Official Journal of the European Union, 2016).

In practice, the personal data refers to any data that can be assigned to a person in any way (e.g. phone number, (IP) address, personal number, account data etc.). Always when processing of personal data, the GDPR applies.

EU also addresses the questions related to the use of online applications. According to the Regulations, *"Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them"* (Official Journal of the European Union, 2016).

Sensitive personal data

Personal data protection is a term closely related to privacy, so both are used in connection with the GDPR. One of the subcategories of the personal data is **sensitive personal data**. This can refer to e.g. information related to a person's origin, health, race, political views, religion. This type of data needs high level protection.

The right to process personal data

A company or organization only has the right to process personal data in case

- the user has given the consent to use the personal data or
- the company/organization needs the personal data in order to fulfill its obligations described in a contract / a law or due to a legitimate interest
- personal data is needed to protect common interests or fundamental interest of the person

Privacy statement

The GDPR requires that the registrar (company / organization) informs the registered user on what personal data is collected and how this data is being processed. The user always has the right to request this information. A privacy statement is not required by the Regulation. However, a privacy statement is a convenient way to inform all registered persons about the p. Typically a privacy statement includes following information

At minimum the following information must be given to the registered persons:

- who processes the personal data
- why this data is collected and processed
- what is the legal basis for processing the data
- who receives the data

In some cases more detailed information is required.

Resources

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the European Union, 2016)
- Reform of EU data protection rules (European Commission 2023).
- What is GDPR? (Horizon 2020, 2023)
- How universities have to adapt under the new EU General Data Protection Regulation (GDPR) (Tattersfield, 2023)

Higher Education Institutions and GDPR

Managing Data and Monitoring User Activity

Every higher education institution should take care of the protection of personal data of its students and control the possibility of access of each individual person or entity. Technology makes access to student data relatively easy, so various measures need to be maintained to keep confidential data secure.
When taking measures to protect the data of their students, higher education institutions (HEI) should consider the following measures:

- Reduce the amount of information collection
- Monitor and protect institutional networks
- Train employees and teaching staff
- Establish criteria for deleting unnecessary information
- Encrypt electronic data
- Enable the anonymity of students when publishing results
- Publish data protection policies, procedures and protocols.

Every institution of higher education should maintain a record keeping policy and clear standards that regulate the method of data storage, the duration of storage with regard to individual categories of data, as well as the method of their storage (e.g. evaluations of individual courses, records of exercises, notes on student activities, etc.) Data storage periods can be longer or shorter, depending on the type of information (in principle between 1 and 7 years after the student's graduation).

Higher education institutions should also pay special attention to the use of mobile devices in classes and while students are in the premises of the institution, such as laptops and smartphones, which provide the possibility of hacking sensitive data. Therefore, it is recommended to use a secure email service with HTTPS encryption, as well as encrypt files with confidential information.

Teachers should be careful when keeping confidential information about students, giving access to the information they keep, and avoid discussing student records with others, unless they have a legitimate need (meetings of teachers within the Department, applications to the Ethics Committee about problematic students, etc.). Also, when teaching, if we present examples of student works, it is necessary to use neutral images and avoid personal data (name and surname) that reveal the student's identity, except in the case we have their written consent. If live data is important, you can obfuscate or blur sensitive information.

Educating students on privacy

With the increasing use of the Internet for learning and teaching, there is an increased risk of students becoming victims of cybercrime, which can include fraud, identity theft, stalking, bullying, email scams, forgery and identity theft. Therefore, it is necessary to warn students about these risks and familiarise them with ways to protect themselves, their privacy and their devices.

Students can take various precautions to protect their data on mobile devices, such as:

- Regularly update mobile devices and applications, avoid unknown websites, delete and report suspicious emails.
- Optimize their operating system, browser and security software regularly;
- Connect all home devices to the Internet via a secure Wi-Fi network;
- Use strong passwords and two-factor authentication;
- Pay attention to the publication of sensitive personal information when using social media.

Resources

Articles

- Data Privacy Assessment: An Exemplary Case for Higher Education Institutions (Habbabeh, Schneider & Asprion, 2019.
- Preparing Students for the Era of the General Data Protection Regulation (GDPR) (Gligora Marković, Debeljak & Kadoić , 2019).
- Understanding Student Privacy and Protecting Their Information (Keeter 2021).

Video clips:

- GDPR Guidance for Schools (Department of education, 2023)
- GDPR Awareness for School Staff (GDPR in Schools - GDPRiS, 2023)

Use of images & videos in universities

Also a photo or a video of a person is a personal data. That is why higher education institutions should pay special attention to the treatment of images, videos and recordings that are the subject of personal data protection. Typically image records are used in higher education in various situations, from online classes that are usually recorded so that they are available to students later, through publications, websites and social media. Such photos and recordings may not be publicly published or used on institutional websites/profiles or on social networks, if they reveal the student's identity, except in the case that the institution has the student's written consent (for each medium separately).

In case it is impossible to collect written consent on the persons appearing in photo / video materials, it is necessary to inform all participants in advance by including a notice in the invitation that the event will be digitally documented..

Recording lectures

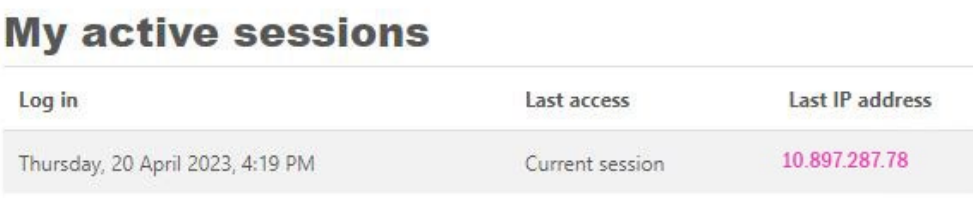
The same requirements apply to the creation and publication of HEI video materials. Students should be warned in advance of the intention to record the lecture (as well as of the recording being available for later viewing). The teacher can ask the student to identify him/herself at the beginning of the lesson, but he/she cannot ask that his/her camera be turned on during the recording of the online lecture. Students

should also be informed if the chat /or other ways of online communication (*whiteboards* etc.) is going to be saved and for what reason. The platform through which lectures are recorded should protect the privacy of students by preserving the confidentiality and security of their personal data in accordance with the GDPR.

Moodle & GDPR

Also Moodle collects personal data. The data can be collected based on consent, contract, legal right or legitimate interest. Users always have the right to request a copy of the information that Moodle or the HEI holds about them. Typical data collected through Moodle are student's name, email, user account, content created by the student such as assignments, comments as well as log data. The issue of collecting Moodle learning analytics is a complex one as this data is quite detailed and sensitive to a certain extent.

Read more: https://moodle.com/privacy-notice/



Moodle collects data e.g.on browser sessions of the users

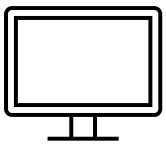
Best practices

- Privacy Notice for the Moodle learning environment (University of Jyväskylä, 2021)
- Guidance on Images and videos concerning GDPR (London's Global University, 2019)
- FAQ GDPR AND EDUCATION (The University of Twente, Netherlands, 2023)
- GDPR for students (Karlstad University, 2023)
- Student Guide to GDPR (University of London, 2023)

GDPR and student evaluation

The issue of privacy and the sharing of sensitive personal data should be regulated in advance by the study contract of each educational institution with its students. Every educational institution has the obligation according to its national legal framework to collect and keep records of examinations (including records of attendance, activities, engagement and work of students, details of passed tests or exams and elements of the final grade). Teachers are obliged to evaluate their students' work transparently according to pre-published criteria, but students should also be informed about the method and length of storage of individual evaluation elements.

According to the article 5 of GDPR Regulations, *"Universities shall process personal data based on the confidentiality principle , i.e. students' data should be secure from unauthorised access and made available on a "need-to-know" basis with teachers. Making a student's full record available to any teaching faculty would be against the data minimization principle, since their grades do not constitute necessary information for teachers to conduct classes."* Based on the above-mentioned principles, it is necessary to request the student's consent for members of the faculty staff even when processing data for the purpose of mentoring. Teachers should determine in advance the procedures related to the handling and access to confidential documents with everyone involved in certain procedures (committee exam, application of the topic of the final paper, etc.).



Resources

How to process personal data in virtual learning

- A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom Aliyu, Maglaras, He, Yevseyeva, Boiten, Cook & Janicke, 2019.
- Privacy and E-Learning: A Pending Task (Alier, Casañ Guerrero, Amo, Severance & Fonseca, 2021).
- Personal Data and Privacy Protection in Online Learning, Guidance for Students, Teachers and Parents, June 2020, Version 1.0, Sart Learning Institute of Beijing Normal University (Huang, Liu, Zhu, Chen, Yang, Tlili, Fang & Wang, 2020).
- Understanding Student Privacy and Protecting Their Information (Keeter, 2020).
- Preparing students for the era of the General Data Protection Regulation (Marković, Debeljak & Kadoić, 2019)

GDPR and cloud services

- For Learning Analytics to Be Sustainable under GDPR—Consequences and Way Forward (Karunaratne, 2021).

GDPR in social media

- Common Sense Education: Learn how to keep student information confidential on social media (Higgin, 2022)
- School posts on Facebook could threaten student privacy. The Conversation. (Rosenberg, 2022)
- Taking photos at school events – Where common sense comes into play (Data protection commission Ireland, 2019).
- GDPR in Moodle. Moodle, 2023.

Other topics

- A brief guide to GDPR for schools and teachers (School Education Gateway, 2018)
- A guide to GDPR for universities (Winqvist, 2023)
- The GDPR and higher education - a debate by a panel of GDPR experts (Damásio, 2023)