INFORMATION NOTICE

on the data protection and data security aspects of digital distance learning at the Faculty of Law and Political Sciences, University of Szeged[1]

I. Personal Data

According to the definitions of the General Data Protection Regulation (GDPR),[2] directly applicable in Hungary from 25 May 2018, personal data means any information relating to an identified or identifiable natural person ("data subject").

Within the frame of distance learning, **personal data**[3] include:

- **the student's name and other identifying data, the content of written and oral assessments, in-class contributions, grades, photograph, any video recording made of them, as well as exam results;**
- **the lecturer's voice and image provided during classes, consultations, or video lectures as well as data relating to their work activities**.

Any operation performed on personal data constitutes **data processing**,[4] which is subject to the GDPR.

II. Data Processing and Data Controllers

In digital distance learning, the purpose of data processing is to ensure higher education in accordance with Act CCIV of 2011 on National Higher Education. Such data processing is **not considered processing for private purposes**, as its clear purpose is to conduct distance learning and perform the tasks defined by law as public duties.

a) **Regarding students' personal data, the data controller**[5] **is the University of Szeged, Faculty of Law and Political Sciences**. The **lecturer** acts in the name and on behalf of the institution and **is bound by confidentiality** with respect to any data concerning students. If personal data are used for purposes other than fulfilling public duties – such

[1] The Information Notice was prepared based on the NAIH's Information Notice on Data Protection and Data Security Aspects of Digital Distance Learning issued on September 30, 2020 (Case No.: NAIH/2020/7127/).
[2] 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)
[3] Art. 4 (1) GDPR: '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.
[4] Art. 4. (2) data 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
[5] Art. 4 (7) controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

as unauthorised disclosure, dissemination, publication, or storage beyond the necessary period – or if security measures are not taken, such actions may constitute unlawful data processing and, in certain cases, a criminal offence.

b) **Students, in respect of data concerning lecturers** (see in I/b.) **and their fellow students** (see in I /a.), **are also considered data controllers**. The GDPR does not apply to personal data processed solely for personal or household activities unrelated to professional or commercial activity ("household exemption").[6] However, **if students use such data for purposes other than participation in education or their own learning** (e.g. by forwarding, distributing, or publishing lecture materials, video lessons, or class recordings) or fails to take measures to ensure data security, such behaviour may also constitute unlawful data processing and, in certain cases, a criminal offence.

III. Legal Basis of Data Processing

If processing personal data is strictly necessary for achieving a specific educational purpose, **the data controller must determine the exact purpose and the legal basis** for processing in accordance with Article 6(1) GDPR.

According to the Hungarian National Authority for Data Protection and Freedom of Information (NAIH), the Faculty of Law and Political Sciences processes data for distance learning on the **legal basis set out in Article 6(1)(e) GDPR** (task carried out in the public interest), meaning that consent is not required.

If a **student** wishes to use the personal data of lecturers or fellow students for purposes unrelated to learning, they **must obtain consent** in accordance with Article 6(1)(a) GDPR.

IV. Principles of Data Processing

Article 5 GDPR sets out the **principles** of data protection, which must always be applied. Thus, personal data may be processed **lawfully and fairly**, and for specified, explicit and **legitimate purposes**. The data controller specified in point II is responsible for compliance with data protection principles and must be able to **demonstrate such compliance** ("accountability").[7]

In accordance with the principle of **data minimization**, only data that is strictly necessary and proportionate to the purpose may be processed. For example, if a student must submit a video to verify a practical task, the recording should show as little as possible of their private living space and no other individuals.

If the same objective can be achieved by methods that do not require personal data, these should be preferred. Less intrusive alternatives – such as real-time online video chats instead of recorded submissions – are recommended where feasible.

In some cases, for example, instead of making and uploading video recordings to monitor the fulfillment of study obligations, using a method of real-time communication (such as online video chat) can be an effective and less risky solution for privacy, provided that the data controller considers alternative solutions to be suitable for achieving the objective.

[6] Art. 2 (2) (c) of the GDPR, having regard to recital 18 of the GDPR
[7] Art. 5 (1)-(2)

Live streaming of classes, focusing primarily on the lecturer and teaching materials, is another less intrusive option. Students should not record or store such broadcasts, as misuse (e.g. online harassment) may occur. Unauthorised recording or use by a student participating in distance learning entails sole liability for any copyright, data protection, or criminal consequences (see II/b.).

If pre-recorded lectures or materials are shared on the designated educational platform, **students become data controllers with corresponding GDPR responsibilities** based on the information contained in this notice, in particular that described in Section II. b).

Under **the storage limitation principle**, video assignments must be kept only as long as necessary. Best practice is to delete them immediately after grading. The controller cannot justify prolonged storage simply for possible later verification.

The Faculty of Law and Political Sciences ensures **transparency** under Articles 13(1)-(2) GDPR through this notice and a separate student data protection notice, which also covers data subject rights under Articles 15–22 GDPR.

The student concerned is entitled, **for reasons related to his or her own situation, to object** to the manner and practical implementation of certain data processing operations carried out in the course of performing public tasks. The educational institution is obliged to examine the objection on its merits, and when assessing it, the data controller must consider whether a less restrictive means of data processing that is less intrusive to the privacy of the data subject can be used to achieve the purpose of the data processing. For example, in the case of online classes or lectures, the objection of a person participating in person must be assessed in such a way that data processing is not more risky for them than their personal participation in a traditional class (see: adjusting the camera angle during class tests), **but it must not lead to the educational institution being unable to perform its public duty in the form of digital distance learning in general.**

V. Data Security Requirements

Under the principles of **confidentiality and integrity**, recordings must be protected against unauthorised access. The Faculty of Law and Political Sciences as the data controller uses closed, internal university systems for teaching, material sharing, administration, and assessments.

Students are responsible for ensuring data security in handling educational materials and personal data of lecturers or peers. Furthermore, it is the student's responsibility to ensure that they have the appropriate technical arrangements in place to participate in teaching and assessments in an appropriate and uninterrupted manner.

It is important for both lecturers and students to comply with basic security requirements, such as using licensed software, antivirus software and virus scanners, and continuously downloading necessary updates. If multiple people use a device, it is important to create separate user accounts, to set and enforce “strong” password requirements, and to use automatic logout after a certain period of inactivity in systems that contain personal data.

The **lecturer** is obliged to use the digital devices at their disposal safely, regardless of whether they are their own devices or have been provided by the educational institution. Given that the

teacher also performs data processing operations necessary for their teaching tasks on their own devices within the scope of the educational institution's responsibility, the institution may request information about the data security measures applied and, if necessary, may also verify them.

Lecturers must use secure digital tools, preferably institution-provided closed platforms, for classes, material sharing, and assessments. Publicly accessible sites may only host materials that do not involve personal data processing.

VI. Remote Assessments and Examinations

If students must submit video proof of a task, the closed university platform should be used. Messaging apps (Messenger, Viber, WhatsApp, etc.) must be avoided. If e-mail submission is exceptionally allowed, the lecturer must delete the file immediately after grading.

Copying videos to external media is discouraged unless no other access is possible, in which case password-protected or encrypted storage must be used to prevent data breaches involving personal data.

For online exams, students may be required to confirm their identity via webcam and keep it on throughout the exam to prevent cheating. Camera angles must avoid showing unnecessary details of the home environment. Storage of such recordings must follow the same principles outlined above.

The storage limitation principle applies to assignments and exam papers, which should be retained only as long as in regular (non-distance) education. For example, after the assessment, the lecturer may retain the data in accordance with the relevant rules of the educational institution, in the case of final exams, thesis defenses, etc.

Szeged, 19 August 2025

Dr. habil. Szilvia Váradi Kertészné, Ph.D.
Data Protection Officer, Assistant Professor