Case number NAIH/2020/7127/

Information
on the data protection and data security aspects of digital distance learning

The extracurricular digital education introduced during the first wave of the Covid-19 pandemic gave rise to a number of data protection and data security issues, particularly in relation to the uploading, sharing and storage of teaching materials, video recordings that verify completion of the students' tasks and other documents. The Hungarian National Authority for Data Protection and Freedom of Information (hereinafter: the Authority) regarded the elevation of data protection awareness as a task of outstanding importance by way of statements published in its website among the institutions as well as the teachers, educators, speakers, trainers (hereinafter jointly: educators) and parents in this field. Because of the rapid proliferation of the pandemic during its second wave, increasing numbers of educational institutions decide again to introduce digital education. In view of the topicality of the subject matter, the Authority is issuing the following information concerning the data protection and data security aspects of digital distance teaching.

I. Based on the definition of the General Data Protection Regulation[1] (hereinafter: GDPR), which is directly applicable also in Hungary as of 25 May 2018, **personal data**[2] means any information relating to an identified or an identifiable natural person ("data subject").

Based on the above, **the name of the pupil or student, his or her other identification data, the content of their written and oral assessments, contributions to classes, results, photos as well as their test and examination results** qualify as personal data and any operation carried out with the data qualify as data processing[3].

It is important to underline that in data protection regulation, **children merit specific protection with regard to their personal data[4]** as they may be less aware of the consequences and risks in relation to the processing of personal data.

Similarly, the voice and image of the educator in relation to what he or she says in the digital class and the data related to his/her workplace activity also qualify as personal data.

II. Currently, there is no legal regulation providing for the framework and detailed rules of digital distance teaching, yet in view of the situation created by the second wave of the coronavirus pandemic – in consideration of the obligations specified in Section 5(3) of Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information (hereinafter: Privacy Act) – legislation in this area continues to be warranted. **Institutions of primary, secondary and tertiary**

---

[1] 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).
[2] GDPR Article 4(1): *"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 on-line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.
[3] GDPR Article 4(2): *"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*.
[4] GDPR Recital (38).

education (hereinafter jointly: educational institutions) may process personal data only subject to the principles of data protection in compliance with the ethical rules, **recommendations, guidelines and other documents of the sector until the legislator regulates the subject matter in detail.**

The provisions of the General Data Protection Regulation do not apply to the processing of personal data by a natural person **in the course of a purely personal or household activity,** which cannot be associated with any professional or business activity (**processing for a private purpose**)[5].

As in the case of digital distance teaching, the purpose of processing is the provision of education and schooling as the basic task of public education pursuant to Act CXC of 2011 on *National Public Education* (hereinafter: Public Education Act)[6] and providing tertiary education according to Act CCIV of 2011 on National Tertiary Education, processing activities carried out in the course of these **do not qualify as data processing for a private purpose** in the opinion of the Authority, because their clear objective is ensuring the continuity of education and schooling as performing a public task specified by law.

Hence it is not the educator, but the **educational institution** having an independent legal personality – **in some cases, the school district provided that it specifies a concrete processing purpose – which shall be regarded as controller**[7], that has to specify the purpose and instruments of data processing, and **its task is to provide appropriate information on processing and to ensure compliance with the other data protection requirements.**

The educator acts as the employee/on behalf of the educational institution and performs a public task. The educator is subject to an **obligation of confidentiality** with respect to the data that have come to his/her knowledge in relation to the child[8]. In the event that he or she uses the personal data processed for any purpose other than that of processing, i.e. the performance of his/her public task (thus, for instance forwards the data to a third party without being authorised to do so, disseminates or publishes the data), or stores the data for a period longer than absolutely necessary, fails to take action to ensure the security of the data, such a behaviour may qualify as unlawful processing, in some cases even a crime.

III. Article 5 of GDPR contains the **main principles**, which **must be complied** with in the course of processing personal data irrespective of the legal basis of processing, which must be continuously enforced in the course of processing. The controller is responsible for compliance with the principles of data protection, and in addition, it must be able to **demonstrate this compliance** ("accountability").[9] Accordingly, the controller shall document and keep records of processing so as to enable the demonstration of its lawfulness after the event.

III.1. The principle of **data minimisation**[10] requires that only data indispensable for the purpose and proportionate to it may be processed (collected and stored). Thus, for instance, if a student has to verify the performance of a school task (primarily of a practical nature) with a video recording, it is expected that no person other than the student be shown in the recording and as little as possible is shown of the private space of his home.

---

[5] GDPR Article 2(2)(c) in view of GDPR Recital (18).
[6] First sentence of Section 7(5) of the Public Education Act.
[7] Sections 41-44 of the Public Education Act.
[8] Section 42(1) of the Public Education Act.
[9] GDPR Article 5(2).
[10] GDPR Article 5(1)(c): *"personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation")."*

It is an important expectation that the processing of personal data may be justified only if the purpose of processing cannot be achieved through **instruments not requiring the processing of the data;** when processing personal data, it is necessary to examine in every case whether there is an efficient **solution that poses less risk to the privacy of data subjects.**

In some cases, for instance, instead of making and uploading a video recording to verify the performance of study obligations, the performance of such obligations could be verified in writing by the parent, or the **use of a method for real time communication** (such as on-line video chat) may be an efficient solution that poses less risk for the privacy of children, if according to the opinion of the controller, these methods are also suitable for achieving the objectve based on the number of children taught and the teaching hours of the educator.

Another less restrictive solution is the **streaming of classes in real time** for students joining in the distance education. The Authority calls attention to the fact that in view of the principle of data minimisation, the camera should be set up so that it should show primarily the educator and the teaching instruments (blackboard, projector) used by him and students should be shown if possible only if it is closely related to the presentation of the activities in class and is necessary for the elaboration of the teaching materials (e.g. presentation of the results of solving a task in a small group for the other students). In view of the principle of purpose limitation, another related requirement is that the classes or lectures streamed should not be recorded or stored because they would not be stored within the framework of traditional education and such recording could be suitable for the abuse of students or educators (for instance, eventual risk of on-line harassment). If a student participating in distance education or the person exercising parental supervision records the real time streaming and uses it without being authorised to do so, he or she will be independently accountable for the legal consequences under copyright law, data protection law and eventual criminal law.

III.2. If the processing of personal data seems to be indispensable for achieving the concrete educational purpose, the controller must first **specify the accurate purpose of processing and the legal basis substantiating the lawfulness of processing**, which in the general cases of processing personal data may be carried out with reference to legal basis according to GDPR Article 6(1)[11].

According to the position of the Authority, it is not the consent of the data subjects (or the person exercising parental supervision in the case of children below the age of 18) [GDPR Article 6(1)(a)][12] **that serves as the legal basis of processing at the educational institution as**

---

[11] GDPR Article 6(1): *"The processing of personal data shall be lawful only if and to the extent that at least one of the following applies:*
a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child.
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.."

[12] The Authority underlines that voluntariness is also missing from the elements of consent as participation in education is an obligation for the pupil or student; in addition, the provision according to Article 8(1) of GDPR cannot naturally be applied to processing.

controller, but **the legal basis specified under GDPR Article 6(1)(e) (performance of a public task), thus the consent of the data subject is not required for processing to be lawful.**

III.3. Pursuant to **the principle of storage limitation**[13] in the case of making a video recording set as a home task, the period of storing the videos sent or uploaded by the students (or the person exercising parental supervision) may not be unlimited; it has to be restricted to the period that is absolutely necessary. According to the opinion of the Authority, a good practice is when the educational institution requires the educator to immediately erase the recordings after the assessment in a way that it cannot be restored. The controller may not refer in general to the fact that the recordings may have to be stored longer because of subsequent supervision to justify additional storage as school supervisors and heads of institutions are not generally present in class.

III.4. Controllers have also to provide for the **transparency of processing and the accuracy of the data.**

The Authority underlines that the controller, i.e. the educational institution, is responsible for **providing the information** according to Article 13(1) and (2) of GDPR to **the data subjects** concerning the circumstances of processing (including the use of digital instruments and the processors made use of in the course of this as addressees), and **it has to develop a detailed privacy statement for them** and **it has to ensure that they can exercise their rights according to Articles 15-22 of GDPR.**

The data subject (or the person exercising parental supervision) **has the right to object to** the mode of certain processing operations and their practical development implemented in the course of discharging a public duty for reasons **related to their own situation (or that of the child supervised by him or her).** The educational institution has to examine the objection in merit; when evaluating it, the controller must consider whether an instrument or processing method that is softer and less restrictive of the privacy of the concrete data subject can be applied to achieve the purpose of processing. Thus, for instance, in the case of a class or lecture streamed on-line, the objection of a person participating in it should be evaluated so that the processing should not be riskier for him or her than his or her personal participation in traditional class (see: setting up the camera); this, however, must not lead to preventing the educational institution from discharging its public duties in the form of digital distance teaching in general.

III.5. Pursuant to **the principles of confidentiality and integrity**[14] when video recordings are stored, it must be ensured that no unauthorised third person should have access to them.

In relation to **data security** the controller has to select the method and technology to be applied, bearing in mind the special protection accorded to children's rights and enforcing the built-in and default principles of data protection[15].

The Authority underlines that the choice of the appropriate technology and requiring educators to use it is the responsibility and obligation of the educational institution as controller throughout the course of processing.

IV. In relation to the above expectations, the Authority calls attention to the following data protection

---

[13] Pursuant to GDPR Article 5(1)(e): *"personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of appropriate, technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation");"*

[14] GDPR Article 5(1)(f): "*personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").*"

[15] GDPR Article (25).

requirement[16] and names the following data security measures as “good practice” in line with the information issued by the Polish data protection authority (UODO):

- The Authority recommends that educational institutions create workplace e-mail addresses for the educators and require them to use the workplace e-mail address in the case of communication outside the educational framework systems (e.g. KRÉTA, Neptun, Moodle).

- If the technical conditions are available, secure remote access to the school systems must be ensured. The educator shall be under an obligation to use the available digital instruments in a secure manner, irrespective of whether those belong to the educator or the educational institution made them available to the educator. In view of the fact that the educator carries out the processing of operations necessary for discharging his teaching tasks under the responsibility of the educational institution , the institution may ask for information about the data security measures applied and if necessary, may oversee them.

- If the educator uses his own device, compliance with basic security requirements such as using non-infringing software, anti-virus software; continuous downloading of the necessary updates is an important demand. Its regulation, design and supervision is also within the responsibility of the educational institution.

- If sending data within the educational framework system cannot be implemented, creating uniform e-mail addresses under the domain name of the educational institution for the students can be a good practice in order to avoid students and parents using their own e-mail addresses in the course of digital distance teaching, which could involve forwarding personal data to third countries.

- The Authority does not recommend copying the videos sent in/uploaded by the students (persons exercising parental supervision) onto a data medium; it may be justified but only in the case if access to the documents cannot be achieved through the educational framework system or through access to the workplace e-mail address. In the event that such copying is indispensable, the use of data medium that is equipped with technical protection (password protection or data medium with file level encryption – hardware encryption) is recommended with a view to preventing data protection incidents affecting the data of children. Such solutions are available free of charge for both parents and educators.

- If students have to verify the performance of a practical task by way of sending a video recording to the educator and the educational framework system is not suitable for this, a solution that is more aware of the data protection aspects than sending through Messenger, Viber, Whatsapp, etc. or e-mail, which can currently be regarded as the most widespread, may be the use of a platform or a dedicated application where the child (the person exercising parental supervision) sends the link to the video uploaded to his/her own account to the educator, which is available for a limited amount of time; after the expiry of the specified period the educator cannot access the video.

- Examinations where the examinee has to verify his/her personal identity through a camera and the examinee is monitored through the camera throughout the examination in order to avoid fraud is the most frequent in the case of institutions of tertiary education. In such cases, it is an important data protection requirement that monitoring through the camera may not involve infringement on privacy, hence the cameras have to be set up so as to show only the relevant data and neither the environment, nor the home, nor the furnishing. The data protection principles detailed above must be enforced also in safeguarding the storage of the recordings.

- In relation to assessments and essays, the principle of limited storage must be enforced as well, thus the period of the storage must be adjusted to such periods required under normal educational

[16] https://uodo.gov.pl/en/553/1118

regimes. Thus, for instance, after assessment the educator may keep the data only in the case of finals, special essays, etc. in accordance with the relevant rules of the educational institution.

- The supervision of educators by the educational institution may be governed by the same rules as in the case of traditional education, the extent of the supervision may not go beyond them. In view of the fact that the head of the institution or the supervisor does not participate in every class even in the case of supervision of traditional education and does not make copies of the works of the students, hence it is not to be expected that the educator keep all the digital materials of the classes and all the works of the students for the purposes of workplace supervision in the case of digital education.

- If an instrument is used by more than one person, it is important to require the use of “strong” passwords or, for instance, applying automatic logout in the event of inactivity for a certain amount of time in systems that also contain personal data.

- The educator should upload only educational materials to publicly accessible channels or websites; they should not be used for activities concomitant with the processing of personal data.

- When data media are used, the educational institution may only use data media, which provide appropriate guarantees for implementing measures ensuring the compliance of processing with GDPR requirements and the protection of the rights of data subjects[17]. As a good practice, the Authority recommends the use of the services of processors established in the EEA area acknowledging the GDPR requirements as mandatory.

In view of the fact that every educational institution has to appoint a data protection officer, whose highlighted task under GDPR is providing advice on issues of data processing, the Authority recommends that the educational institutions and the educators should consult their data protection officer when developing their activities concomitant with the processing of personal data in order to transpose the above requirements into practice.

Budapest, 30 September 2020

Dr. Attila Péterfalvi
President
Honorary university professor

[17] GDPR Article 28] (1).