PERSONAL DATA PROTECTION OFFICE

Security of personal data during remote learning

With regards to the coronavirus pandemic, e-mail and other elements of group work, such as conference tools or internet communicators, have become aids to many students and teachers, who use remote learning methods. Using these, one must keep in mind the security of data processing.

If you are the principal…

- The schools have found themselves being in an exceptional situation where they must face new demands related to remote learning. New regulations pertaining to conducting classes remotely provide the teachers with far-reaching possibilities to conduct classes using methods and techniques of distance education or other way of education, using inter alia electronic communication. Thus these rules give schools the freedom to choose the most fitting tool, taking into account all the aspects related to the capabilities of the unit, the teachers, and above all – taking into account the technical and organisational capabilities of the parents and students.

- It is the obligation of the school to inform teachers, parents and students about the methods of conducting distance education. This information should be provided in a clear manner so that it is understandable for everyone who is targeted by this announcement. If the school, in order to provide distance education, would use new tools or services offered by external entities, it is obliged to inform on the scope of personal data being processed.

- The school should provide the tools enabling the teachers to conduct classes remotely and to safely communicate with students and their parents – implementing these tools in the unit in a comprehensive manner.

- The school might require the student or his/her parent/legal guardian to provide the data necessary for creating an account in the remote learning system, but only in the scope necessary to create such an account. This occasion should not serve to gather excessive data or data serving other purposes.

- The school which wants to make use of data processing services using tools other that the ones previously used, should first of all – with the help of a designated Data Protection Officer – conduct a risk analysis. Special attention should be paid to data security and to the provision of adequate guarantees of data subjects' rights.

- One of the main obligations of the schools that relate to personal data protection is to safeguard data by implementing adequate technical and organisational measures. These data should not be disclosed to unauthorised persons and should not be destroyed, modified or lost. Exemplary measures to safeguard the data are: pseudonymisation, and data encryption.

- In the event of carrying out their work-related duties by the teachers outside the school premises, the principal must in any case consider the options that allow adequate data protection level, taking into account the level of risk of data protection breaches, and must implement adequate measures to mitigate this risk, or resign from conducting activities that pose such risk,

e.g. allowing the teacher who does not have the conditions necessary to conduct remote work to use the equipment stored in the school premises.

- If the school is outsourcing certain activities, e.g. the service of the electronic school register, the principal must be assured that the service provider is able to ensure sufficient guarantees to implement adequate technical and organisational measures in order for the processing to fulfil the requirements of the GDPR and to protect data subjects' rights. Therefore, before making such decision the school must analyse all the solutions available and assess the risk.

- The principal should not recommend to the teachers the use of their private e-mail addresses for contacting their students or their parents / legal guardians. It is recommended that the teachers use their work e-mails to contact their students. However, in both cases they should be adequately safeguarding the personal data being disclosed in their messages.

If you are a teacher…

- The teacher can process his/her students' and their parents'/legal guardians' data only for the purposes related to executing his/her professional duties.

- The teacher must keep in mind to safely use the computers and other devices both when these were provided by the employer, and when using personal equipment.

- The GDPR does not forbid the use of personal computer, tablet or a telephone for personal data processing related to conducting classes remotely. However, these devices must be adequately safeguarded, and the teacher should comply with the policy or other procedure implemented by the school in this regard.

- If the teacher is using his/ her own device, he/she should independently fulfil the fundamental security requirements. First of all, it is necessary to verify, whether the device being used is equipped with an up-to-date operating system, whether the software is being used, especially antivirus software, and whether the necessary updates were installed. Anti-malware and anti-spyware software should also be kept up to date. It is necessary to install the software in a cautious manner and it should be downloaded only from reliable sources (the websites of their manufacturers).

- When storing the data in the equipment that might be accessed by other persons, it is necessary to use strong passwords, and before walking away from the workstation, you should log out from the device at all times. It is also recommended that automatic logging out should be configured after a period of inactivity as well as creating separate user accounts in the event of usage of the computer by several persons.

- When using the software or mobile applications it is necessary to use all technically possible mechanisms that protect the privacy of the users. If the usage of some of the software requires logging in, it is worthy to care for a strong password, additionally protected from loss and the access by unauthorised persons.

- When data are stored on portable devices (e.g. USB stick), they must be absolutely encrypted and password-protected to ensure adequate security of personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage.

– To a basic extent, communication with students and parents is carried out through ICT solutions implemented by the school, e.g. electronic school registers. In this situation, the teacher must still observe the basic safety rules while connecting to the electronic school register remotely from his/her device at home.

– Conducting classes remotely may require the teacher to use electronic mail to contact students or parents. The teacher should keep correspondence from the official mailbox, which should be provided by the school. If the school has not provided teachers with official mailboxes, teachers must remember that private mailbox should be used for business purposes in a prudent and secure manner.

– Particular attention must be paid to the security of personal data provided in sent messages. Before sending a message, always make sure that it is necessary to send personal data and that it is intended to be sent to the right recipient. In addition, you need to check whether the recipient's e-mail address does not contain, for example, shifted or omitted characters to avoid sending it to unauthorised persons. When sending bulk mail, you should use the "BCC" option so that recipients of the message will not see each other's email addresses.

– In order to conduct distance learning, the teacher should use educational platforms or e-learning tools that have been implemented at school. In such situation, the teacher can expect that conducting classes remotely will be safe. The teacher should follow the school's instructions and procedures for the personal data protection and must maintain basic security principles when connecting to such a platform remotely from his/her device at home.

– The school should implement independently the distance learning method and technique selected from available sources or other tools of performing tasks remotely. Teachers should not decide on the use of specific solutions independently (e.g. conducting classes with the use of messengers or video tools). However, given the extraordinary situation and the urgent need to start online classes, this may be justified in some situations. It should be remembered that it is always the school that is responsible for processing student’s data using tools implemented by the teacher. Therefore, the adoption of a specific solution should be made in consultation with the school principal or the distance learning coordinator appointed by him or her who must be aware of the used tools. This solution should be considered temporary.

– When choosing an application or other tools to be used in distance education or communication with students, it should be always considered whether it is necessary to process personal data, and if so, whether their scope can be minimised or if the nicknames can be used (e.g. the first letter of the name, etc.). You should also check the service provision and data processing rules established by the service provider (privacy policy).

– In the current situation, in consultation with the school headmaster, the teacher should take into account what real options the students and parents have for communicating with the

PERSONAL DATA PROTECTION OFFICE

teacher, provided that the specific type of internet messenger indicated by them ensures the security of communication.

– On publicly available portals or websites, the teacher can publish only educational materials, but he or she cannot process the personal data of students or parents.

– In order to check and monitor the presence of students in remote classes, the teacher should maintain the principles of proportionality and data minimisation. For example, the teacher cannot use the tools that collect biometric data, including face recognition systems.

If you are a parent ...

– The school may require from the student only such data that are necessary to set up an account in the appropriate distance teaching system and in order to fulfil the obligation of distance learning (pursuant to Art. 35 of the Educational Law Act in connection with Article 6(1)(e) of the GDPR).

– A parent (legal guardian) has the right to know how the school as the controller will process his/her child's personal data during distance learning and what rights he or she has.

– If the platforms used for distance learning are data controllers separate from the school, then parents and children should receive from them an information clause about the basic rules and scope of data collection and the controller, e.g. when setting up an account.

NB!
The legal basis for the implementation of distance education is set out in the Regulation by the Minister of National Education of 20 March 2020 on special solutions in the period of temporary limitation of the functioning of units of the education system in connection with preventing, counteracting and combating of COVID-19 (Journal of Laws, item 493).

Source: www.uodo.gov.pl