REPUBLIC OF ALBANIA
PERSONAL DATA PROTECTION COMMISSIONER
OFFICE OF THE COMMISSIONER

INSTRUCTION

No 4, of 16 March 2010

ON

SAFETY MEASURES FOR THE PERSONAL DATA IN THE FIELD OF EDUCATION

Pursuant to Law No 9887, of 10 March 2008 "On protection of personal data", Decisions of the Assembly of the Republic of Albania No 211, of 11 September 2008 "On the appointment of the data protection Commissioner", No 225, of 13 November 2008 "on the approval of the organizational structure and salary scales of the employees of the office of the commissioner for the protection of personal data" an in implementation of obligations arising from paragraph "f" of point 1 of Article 30, of the abovementioned Law;

I HEREBY INSTRUCT:

The taking of security measures and creating of awareness for the protection of personal data in the field of education:

1. In the field of education, personal data are collected directly by the data subjects or custodians thereof.

    - Personal data subject is every subject whose data are processed; pupils, students and all the subjects which have applied in this institution. Personal data are given by custodians of data subjects who may be the parents or custodians as decided final decision of the court.

2. The data subject has the right to be informed on the data which will be processed, including transfers.

    - Information of the data subject includes the purpose of processing, categories of recipients and any other information which is necessary to ensure fair and lawful processing of the data.

3. With regard to the processing of personal data related to diseases, disabilities, medical checks, psychological and educational visits, there have to be in place clear methods of data processing.

    - Methods include the assigning of a safe place where such data will be kept and ensure that data can be accessed only by authorized persons. In cases of automatic processing of data, these methods include: printing and scanning only in specifically dedicated machines and not in the common ones. Copying to be done only when necessary. In cases of transfers, data must be encrypted.

    - Reports or individual files which are kept by specialists of the areas mentioned in point 3 in their course of activity, are excluded from the reporting of information to the respective superiors, pupils, students, teachers and third parties, by making case by case assessments.

4. You should define clear timelines for the retention and erasure of data, when it is no longer necessary.

    - Data will be retained for as long as it will be necessary for the purposes for which it was collected. When they are no longer necessary, they should be destroyed, keeping in mind the need to do it in a secure manner. Therefore, as regards data retention and data security, instructions and decisions of the Commissioner for Data Protection should be taken into consideration and implemented.

5. Ethics plays a crucial role during the data processing. Therefore it is indispensible that the interested parties promote the introduction of security culture.

    - Moreover, introduction of security measures for the protection of personal data is related to the implementation of the confidentiality principle, which means that controllers, processors and persona who come to know the content of personal data during their work activities, are bound to preserve confidentiality even after termination of their function. Breach of confidentiality constitutes a criminal offence set out in the criminal code (article 123).

6. Assessment of the risks needs to take into account factors such as the technical potential, costs, sensitivity of data as well as probability of systems crashing.

    - Risk assessment is done with the purpose of taking measures to minimise the sharing, dissemination or any other action which is in violation to the data protection law. Lowering of the risk, requires an increase of spending in technology (equipment) etc.

7. Policies and procedures must be based on periodic assessments of the security.

8. Personal data protection is achieved amount others, through security measures. They are as follows:

    a) Install and update an antivirus and firewalls which protect computers;

    b) Update the operating system and download the latest release of applications;

    c) Allow staff to have access only in those materials which are needed to perform their tasks.

    ç) Be careful with the use of passwords/;

    d) Encrypt all information which may cause harm if disseminated;

    dh) Specify recovery procedures in case of damage.

9. Awareness-raising is very important in the protection of personal data. This is achieved by informing pupils, students and parents periodically, in connection to the data protection and by organizing workshops on this topic where competent persons could be invited, such as the IT director. It must be clear that security incidents might bring very serious consequences for the data subject.

10. The staff must be appropriately responsive in individual and team roles during the data processing. Consequently, it needs to examine if the policies, practices in place, measures and procedures are in compliance with the data protection principles.

11. The transfer of data belonging to pupils, parents and teaching as well as administrative staff of the schools and responsible bodies, is allowed only provided that this is necessary for the accomplishment of tasks.

    - Tasks, include all the definitions of the legislation in the field of education.

12. Transfer of the personal data of individuals or private organizations must be made only following consent of the data subjects and in compliance with the purpose for which they were gathered.

    - The data subject gives his or her expressed consent for the transfer of such data. The consent must be expressed and clear. The consent might be implied, by filling in an application form or written declaration, which is an expressed and clear form of consent. The consent must be given on a free will, it should be legal and in good faith and the data subject must be well informed.

13. If the data recipient shall transfer the data for a purpose different from the requested one, then he shall request again the data subject to give his consent.

    a) Data recipient is the institution which is given the personal data.

    b) If personal data are to be transferred for a purpose which is different from the one already stated, then it must be ensured that the new purpose is in compliance with all data protection principles. These principles include a processing which is honest, fair and lawful and at the same time guaranteeing the fundamental human rights, in particular, the right to privacy.

14. Every transfer must be registered and documented in a register. Such activities are made in compliance with Decision of the Data Protection Commissioner, based on point 6 of article 27 “Procedures for the administration and registration of data, data entry, data processing and their disclosure”.

Pursuant to point 2 of Article 4 of the Law on Protection of Personal Data, all public and private controllers in the field of education are tasked with the implementation of this instruction.

This instruction enters into force on 16 March 2010 and is published in our official website, www.kmdp.al.

COMMISSIONER

FLORA ÇABEJ (POGAÇE)