REPUBLIC OF ALBANIA
RIGHT TO INFORMATION AND PERSONAL DATA PROTECTION COMMISSIONER

GUIDELINE

No.01, dated 30.04.2025

ON
SECURITY MEASURES FOR PERSONAL DATA IN THE AREA OF EDUCATION

Pursuant to article 82, paragraph 1, letter “d”, article 85, paragraph 1, and article 97, paragraph 2, of Law No. 124/2024 “On Protection of Personal Data” (hereinafter referred to as “the Law”), the Information and Data Protection Commissioner, hereby issues the following,

GUIDELINE:

Article 1
Scope

This guideline aims to define security measures and raise awareness about the protection of personal data in the field of education.

Article 2
Definitions

The terms used in this guideline, shall have the same meaning as those in article 5, of Personal Data Protection Law.

Article 3
General provisions

1. Personal data in the field of education shall be collected directly from the data subjects or their custodians. Data subjects in the field of education are considered pupils, students and all those who are registered in an educational institution. Their personal data shall be provided by them, when at adult age, or by their parents or legal custodians, when they are minors.

2. Data subjects, have the right to be informed about the data that will be processed[1]. The controller must provide any information and carry out any communication pursuant to articles 13 - 20 of the Law, on the processing of their data in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular as regards information specifically addressed to a minor.

Article 4
Sensitive personal data in the area of education

1. Personal data related to health status, different ability, medical check-ups, psychological visits in school premises, are treated as sensitive data[2] which are processed only in accordance with article 9 of the Law.
2. For the storage of these data, it is important to determine the secure places where such data will be kept, ensuring that they can only be accessed by authorized persons. In cases of automated data processing, printing and scanning should be carried out only with equipment for specific and non-common use. Copying of data should be carried out only when necessary. When processing is carried out through data transfer, they must be encrypted.
3. Professionals engaged in the fields mentioned in paragraph 1 of this article, during the exercise of their work activity, must not disseminate information which they come into contact with from individual reports or files, to other pupils/students, teachers or third parties, except when this processing process is carried out due to the vital interest of the data subject, in accordance with letter "c" of article 9 of the Law.

Article 5
Processing of personal data in the area of education

1. Data processed in accordance with the provisions of article 6 of the Law may be stored for as long as is necessary for the purposes for which they were collected. If the stored data are no longer needed, they must be deleted, anonymized or destroyed by implementing appropriate security measures.
2. Ethics plays an essential role in data processing. Respect for the principle of integrity and confidentiality under article 6, paragraph 6 of the Law is important to apply whenever personal data are processed. Controllers, processors and personnel who become aware of the content of personal data in the course of their professional activities are obliged to maintain confidentiality even after the termination of their function.

[1] Pursuant to article 13, of Law no. 124/2024 *"On Protection of Personal Data".*

[2] Article 5, paragraph 28 of the Law states: *"Sensitive data*" *are special categories of personal data revealing racial or ethnic origin, political opinions, religious beliefs or philosophical views, trade union membership, genetic data, biometric data, data concerning a person's health, life or sexual orientation."*

Article 6
Security measures

1. It is the controller's duty, that taking into account technological developments, implementation costs and nature, scope, context and purposes of the processing, as well as the risk level for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

2. These measures shall consist, inter alia, of:

   a) pseudonymisation and encryption of personal data;
   b) the ability to ensure the confidentiality, integrity, availability and resilience of the processing systems and services;
   c) the ability to restore the availability and access to personal data within a reasonable time in the event of a physical or technical incident;
   ç) a process for regularly testing, reviewing and assessing the effectiveness of the technical and organisational measures to ensure the security of the processing;
   d) the installation and updating of computer protecting antivirus and firewalls;
   dh) updating the operating system and downloading the latest versions of applications;
   e) allowing staff to have access only to the materials that are necessary to perform their tasks;
   ë) diligence in passwords use.

In assessing the appropriate level of security, the risks posed by the processing, in particular accidental or unlawful destruction, loss, alteration, unauthorized dissemination or access to personal data transmitted, stored or processed in any way, shall be taken into account.

3. Awareness is very important in the function of personal data protection. This is achieved by informing pupils, students and parents periodically through the development of training on this topic, also inviting professionals in the field of information technology.
4. Security breaches events may bring very serious consequences for the personal data subjects. In the event of a personal data breach, the controller shall notify the Commissioner as soon as possible, but not later than 72 (seventy-two) hours after becoming aware of the breach. If the notification is not made within these deadlines, the controller shall provide the Commissioner with the reasons for the delay in notification.
5. The notification to the Commissioner, pursuant to paragraph 1 of this article, must at least:

   a) describe the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects, as well as the categories and approximate number of personal data accounts affected;
   b) communicate the name and contact details of the data protection officer or other point of contact;
   c) describe the possible consequences of the personal data breach;
   d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

6. Staff must be act responsibly by acting promptly and appropriately when processing data. For this reason, it is important to review policies, practices, measures taken and procedures followed to ensure that they fully comply with data protection principles.

Article 7
Transfer of the personal data in the area of education

1. The transfer of personal data of pupils, students, their parents or custodians, as well as of the teaching and administrative staff of schools and responsible bodies, shall be allowed only when:
    a) the data subject has given consent [3], which serves as evidence of the manifestation of clear, full and free will, which means that the data subject has been informed of the reason for the processing and expresses consent to the processing of personal data belonging to him/her for one or more specific purposes.
    b) it is necessary for the fulfilling and implementing the tasks determined by the legislation in the field of education. The data are not processed for a purpose other than the initial one[4] determined at the time of collection. If the data are to be transferred for a purpose other than the initial one, the data subject must again give consent for this new purpose.
2. If personal data are to be transferred for a different purpose, the controller must ensure that the new purpose is also in compliance with all data protection principles and the provisions of Law no. 124/2024 "On Protection of Personal Data" and must ensure that the data subject has again given consent for this new purpose.
3. Each transfer must be documented in accordance with article 27 of the Law.

Article 8
Final provisions

1. All public and private controllers/processors in the territory of the Republic of Albania, which exercise activities in the field of education, shall be responsible for the implementation of this Guideline.
2. Failure to implement the requirements of this guideline constitutes a violation of Law no. 124/2024 "On Protection of Personal Data" and is punishable in accordance with article 94 of this Law.

[3] Article 5, paragraph 14 of Law no. 124/2024 "On Personal Data Protection", states that: *"Consent" is any freely given, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by any other unequivocal affirmative action, expresses agreement to the processing of personal data relating to him or her for one or more specific purposes".*

[4] Article 5, paragraph 17 of Law no. 124/2024 "On Personal Data Protection", states that: *"Further processing" is the processing of data for a purpose other than the initial one determined at the time of data collection, including the transfer or making available of data for this new purpose".*

3. Guideline no. 4, dated 16.03.2010 “On Taking Personal Data Security Measures in the Field of Education” and Guideline no. 7, dated 09.06.2010 “On Personal Data Processing in Higher Education Institutions”, shall be repealed.

This Guideline shall enter into force upon publication in the Official Gazette.

COMMISSIONER

Besnik Dervishi