IMPLEMENTATION AND APPLICATION OF GDPR IN ROMANIAN EDUCATIONAL INSTITUTIONS

Anișoara BELBE
Phd student, Accounting, Doctoral School of Economic And Humanities, "Valahia" University, Târgoviște, Romania, e-mail: a.pavelescu.dc@valahia.ro

***Abstract**: Today, in Europe, more than 250 million people use the internet every day, both to visit social networking sites or platforms and to make purchases, bank transactions or tax returns in electronic format. The multitude of online activities carried out imposed a regulation of the circulation of personal data. According to Eurostat data, 85% of Romanians offer their personal data online, without thinking about the consequences, as opposed to 20%, which is the European average. We are therefore a vulnerable people, despite the fact that personal data trafficking has become a common practice in recent years. However, data security does not only target the virtual environment, but also the physical one. Thus, many public or private institutions and companies that take over and process personal data have to comply with the new Regulation. Of all the personal data processing institutions, we will direct our research to the educational units in Romania, as the situation is much more sensitive, considering the data subject - the minor. The purpose of this paper is to investigate the consequences of applying the GDPR one year after implementation, in pre-university education units in the country.*

Keywords: GDPR; educational institutions; personal data; protection.

Classification JEL: A12, O30, I21

1. Introduction

In a world governed by change, which is becoming more and more complex and connected, people are constantly looking to adapt and evolve. However, their basic needs remain the same. Analyzing the pyramid of human needs (figure 1), we can see the important place occupied by the need for security, material and mental protection. Starting from this primary need, people look for solutions to protect themselves from any external threats.

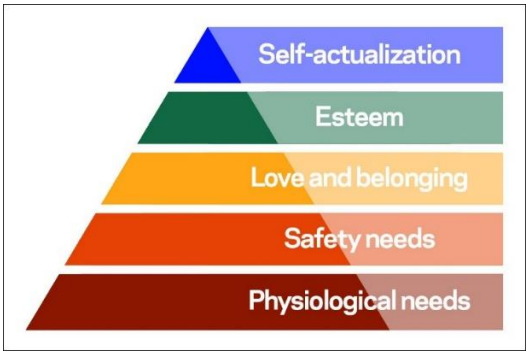

Figure 1: The pyramid of human needs
Source: www.simplypsychology.org

A recent concern for the security of individuals is related to the protection of personal data. Since two decades ago, the European Parliament has shown its involvement in the protection of such data by Directive 95/46 / EC, subsequently repealed by Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of data. of these data (GDPR), applicable in Romania from May 25, 2018.
We will analyze, in the following, how schools have adapted to GDPR, the situations they face, the responsibilities of a data protection officer in a school and the impact that this Regulation has on all educational factors.
The first step taken by educational institutions in Romania after the application of GDPR was the appointment of a data protection officer, also called a data protection officer (DPO - data protection officer). Of course, choosing this person could not be a coincidence. In addition to personal qualities (integrity and ethics), it is ideal for a DPO to have some professional qualities, such as experience in data protection legislation and practices, knowledge of the organization and operation of the school, proper understanding of GDPR and knowledge of technology. computer science. Thus, from the first step, many schools also faced the first problem. Being a field with which they do not intersect every day, the teaching and non-teaching staff received this invitation with skepticism, not knowing if they will be able to adapt to the new legislative changes.
The work of a DPO in a school is voluntary, unpaid and involves a great responsibility, given the multitude of personal data processed. Its role is to advise and inform the director and employees of the educational institution about their obligations regarding the protection of personal data; to monitor compliance with the provisions of the GDPR in the institution and to continuously train employees, in order to adapt to legislative changes; to assume the role of contact person for situations involving the protection of personal data; to communicate with the National Authority for the Supervision of Personal Data Processing; to be involved in school activities properly and in a timely manner.
After the election and appointment of the DPO by the Board of Directors, by a decision, follows a training stage, by participating in training courses. The in-depth study of the Regulation and the Guide issued by the European Commission allows

the data protection officer to apply GDPR at school level, following three fundamental steps: ANALYSIS, IMPLEMENTATION, PRACTICE. Next, we will analyze each step and the impact on the school environment.

1. ANALYSIS

1.1. Personal data

The analysis first involves establishing the personal data that the school collects and processes: name and surname, citizenship / nationality, home / residence address, personal numerical code, date and place of birth, series and no. identity card, photo / video of the person, handwritten signature, e-mail address, telephone number, profession and job, marital status, education and training, school results.

1.2. Categories of people

The following are the categories of persons whose data are processed: students, parents, their legal representatives, other family members, candidates for national tests or exams, future students, teachers, auxiliary teachers and non-teaching staff in contractual relations with the school, candidates for competitions for positions in the education system, any natural or legal person who has commercial or contractual relations with the school.

1.3. Legal basis

As institutions of the MEN, schools "process personal data in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, respectively of art. 6 para. (1) lit. b), c), d), e)", having the obligation to manage the data in secure conditions and only for the specified purposes.

1.4. Purpose of processing

The main purpose for which a school processes personal data is the provision of services in order to achieve the object of activity, namely, education and culture. At the same time, the data can be used for statistical analysis or processing, for substantiating educational management decisions or for archiving, according to the legislation in force. In cases where students benefit from school scholarships, the "Second Chance" program, the "Milk and Horn" program or other programs similarly, the purpose of processing is social protection. If the school is equipped with audio-video surveillance systems, the purpose of image processing is the security of people and monitoring access to public or private spaces. If the data subject has a service or commercial contract with the educational institution, the purpose is the financial-accounting records.

1.5. Motivation for processing

The motivation for which a school collects personal data is related to the need to have information on the basis of which some educational management decisions can be made. Although education in Romania is free, it is necessary for individuals to voluntarily provide some personal data and agree to their storage and processing. Otherwise, schools do not can initiate legal relationships, as they are unable to comply with certain regulations of the education system, and in the case of school employees, labor law and employment law fiscal. At the same time, for better communication with students and their representatives, some schools also collect data that is not mandatory, such as phone number or e-mail address. It can even be considered a security measure for school employees to have access to the phone number of parents / guardians in case of urgent situations involving the student.
Schools can also carry out some statistical surveys, by applying online or telephone questionnaires, in order to improve the educational act. Parents who have given their consent to the processing of this optional data may at any time request the modification or deletion of the data. In the event of a refusal to provide, the school may only transmit information about its services directly.
In cases where persons are included in social protection programs, the provision of data is necessary for access to those categories of programs. For example, in order to receive free supplies, parents of students must prove by a certificate of salary / unemployment / social assistance that they do not exceed a certain income depending on the number of family members. Otherwise, they cannot benefit from that program.
If the school concludes a contract with a natural person, and not a legal person (the data of legal persons are not considered personal data), data are processed in order to comply with the provisions on financial-accounting operations. The refusal of the person in question leads to the impossibility of the school unit to start legal relations.

1.6. Authorized persons and institutions

At the same stage, of analysis, it is necessary to identify the persons within the educational unit who have access to personal data and who process this data, but also the persons or institutions to whom the school can provide data. In a school, the physical security of documents containing personal data is very important, as not every employee should have access to any kind of data. The DPO, the secretary, the accountant, the institution and the management team generally have access to all personal data held by the school, both in physical and electronic format. The administrator and the computer scientist also have access to a certain category of data. Teachers have access to data regarding students and their parents / guardians, data that can be found in the catalog or in the electronic catalog (if applicable). Each school employee must sign a data confidentiality statement.
Schools have the obligation to provide personal data when requested by competent institutions, such as the Ministry of National Education, the County School

Inspectorate, the Teaching Staff House, I.T.M., A.N.A.F., A.J.O.F.M., Police, criminal investigation bodies, other school institutions, respecting legislative provisions.
In cases where personal data is requested by individuals or non-disabled institutions, the DPO will analyze the situation to see if the provisions of the GDPR are violated or not, will fill in the register a request form, will inform the head of the institution, the decision belonging to the latter.

1.7. The rights of data subjects

Educational establishments must take into account the rights of the persons whose personal data are processed and inform about these rights. The school undertakes to offer, first of all, the right of access to the data held, both to the students and to their parents / legal guardians.
Another right that must be taken into account is the right to rectify personal data. Individuals whose data is collected may request a change at any time, both to update information (for example: change of address, telephone number, marital status, family name) and to correct mistakes.
The right to data portability implies the possibility for the data subject to receive in a structured, electronic format all stored data, in order to be transmitted to another personal data controller (usually another school).
The right of deletion or the right to "be forgotten" implies that, in situations specifically regulated by law, the data subject may request the deletion of all data held by the school, which also means the withdrawal of consent to data processing. It should also be borne in mind that certain data are archived in accordance with the law and cannot be deleted. For example, school catalogs are archived for long periods of time, in order to be able to provide information about the school situation of a certain student, in a certain period, if the transcript cannot be accessed. Therefore, in such situations, the right of cancellation cannot be exercised. The regulation provides for several cases in which personal data cannot be deleted: they are necessary for the exercise of the right to freedom of expression; there are legal obligations that require data retention; there are reasons of public interest (purposes of scientific, statistical or historical research). Schools have the obligation to delete illegally collected data without the person's consent. In cases where a specific person requests the deletion of data, anonymization can be used. If the anonymized, encrypted or pseudonymized data may lead to the re-identification of the person, it remains personal data and is still covered by the GDPR. If personal data has been made anonymous so that the individual can no longer be identified, then it is no longer considered personal data.
Other rights of data subjects are the right to lodge a complaint (if the provisions of the GDPR have not been complied with by the school), the right to object to the processing of data, the right to withdraw their consent to the processing of data or the right to anonymization of personal data by encryption or encryption.

1.8. Personal data processed in the computer system

GDPR protects both manually and automatically processed data with the help of computer systems. Regardless of the technique used: in an ICT system, by video surveillance or on literal media, the data processed by a school must be secured. In the age of technology it is almost impossible for personal data not to exist in the computer system of an educational institution. All student data are compulsorily entered in the Integrated Information System of Education in Romania (SIIIR). At the same time, employee data are entered in the payroll system (REVISAL). The data protection officer must ensure that this data is secure and cannot be accessed by anyone in the institution.

In many schools in Romania, electronic catalogs have been implemented, which allow parents / guardians to check the learning situation of students and their absences in real time, based on user and password. For example, if a student is absent from a course, the parent can be notified on the mobile phone, by text message or e-mail, in a very short time. This situation is valid only in the case of one's own child, and the situation of other students cannot be verified by the parent. Students 'representatives must agree to the use of students' personal data on the electronic platform. In case of contract, they cannot benefit from the service described. At the same time, the operators that offer to the school, by contract, this electronic platform must declare that they will not use the database for direct marketing purposes or for other purposes. The DPO must ensure that there are data protection and confidentiality clauses with all third parties with whom the school enters into contracts, in order to assume their responsibility for remote access.

Both a school's website and employees' e-mail addresses must operate on their own domain, owned by the school. Very few schools have complied with these regulations, although the risk of information leakage would be much lower. Employees should not use their personal telephone number or e-mail address in the course of their duties. At the conclusion of the employment / management contract, the telephone and e-mail of the service, non-personal data, must be transferred to the new job holder.

Employees must use the computers provided by the school, holding a dedicated administrator account, as well as a password consisting of at least 8 characters (numbers, letters, symbols and at least one capital letter). These measures do not allow information to leak into the internal or external environment. It is ideal that the Internet access is wired, and if it is wireless, there is a password. It is recommended to uninstall personal software, such as Yahoo Messenger, Orange, etc., which are not related to the activity carried out in the school. The operating systems, antivirus and other programs used must be licensed and require daily up-to-date data. The printers do not have to be in a place of access for the general public, being ideal to be in the same office / same classroom as the terminal.

The person in charge of data protection, together with the institution's computer scientist, must ensure the mapping of the computer systems. If there is a server, the information that is sent to it must be encrypted. All computers in the institution must be networked to the server managed by an external provider. It is recommended to

perform daily backups on the institution's server. The establishment of the degree of information security, the data circuit in the institution and the period of storage of personal data in the computer system must be taken into account.

2. IMPLEMENTATIONS

2.1. Elaboration of the internal regulation on data protection

In order to properly implement the GDPR in the school, the DPO will process an internal regulation on the protection of personal data. This regulation must be known by all employees of the institution, but also by its beneficiaries, being displayed both in the school and on the official website of the school. The regulation should contain some important aspects that refer to the application of the GDPR, namely: general information about personal data; categories of people; the purpose of collection and processing; motivation for collection and processing; parties who have access to personal information; the rights of persons whose personal data are collected and / or processed; special data processing; the use of electronic means of communication in the course of work; breach of personal data security. The regulation must be presented to the Teachers' Council and approved by the Board of Directors.

2.2. Obtaining data processing agreement from employees

At the implementation stage, the data protection officer must draw up an agreement for the processing of employees' personal data by the institution. This agreement must be signed in duplicate by the person concerned. One of the copies will remain with the employee, the other being submitted in a dedicated GDPR file of the DPO. Employees must declare that they have taken note of the provisions of Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and that they agree as an educational institution, as an employer, to store and process the personal data referred to in that agreement (in general, these are first and last name, nationality, domicile / residence address, personal numerical code, date and place of birth, series and number of identity document, photograph / filming, handwritten signature, e-mail address, telephone number, profession and job, marital status, education and training). In the same statement, employees must specify whether or not they want the name, image and footage to be published on the school's website or website. The educational institution has the obligation to inform the employees about the purpose of data processing and the period of their storage. Usually, the period corresponds to the duration of the employment contract that the employee has with the school, subsequently being stored only the data required by the legislation in force. Employees should also be informed about their personal data protection rights (point 2.1.7.), As well as the institutions or persons who may have access to the data.

2.3. Training of school staff

The Data Protection Officer is responsible for instructing all school staff, including the management team, on Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The training is done periodically, both in the implementation phase and in the implementation phase. The DPO must be constantly connected to the new legislation in order to inform the leaders of the school and its employees. The first training involves the presentation of the Regulation and the specific situations of the school to be followed, in order to apply the legislation. Employees need to know what personal data is, what kind of data is processed by the school, what sensitive data is, who has access to this data, what is the legal basis for processing, for what purposes the data is processed, what institutions or persons are empowered to obtain data stored by the school, which involves a violation of the Regulation, how a deviation from it can be notified, what are the risks of data protection in a school and what measures should be taken to prevent information leakage. In turn, teachers have the obligation to disseminate this information to students and their representatives.

2.4. Preparation of employee privacy statements

After completing the first training, the DPO must draw up a confidentiality statement for the institution's employees, in which they assume the assurance of data security, in accordance with the GDPR. As teachers and non-teaching staff have access to personal data of students and parents, they must disclose personal data only to the persons concerned and process them only in relation to the requirements of the job description or the employer. Employees are required to notify the Data Protection Officer in the event of any breach of the Regulation or security incidents.

2.5. Obtaining the data processing agreement from the beneficiaries of the institution

Since enrolling the student in school, some mandatory documents are required that constitute the enrollment file, such as a copy of the identity card of the legal representative or the birth certificate of the student. Thus, if the beneficiaries do not agree to make these documents available, they cannot conclude an educational contract with the respective school.
Next, the DPO will develop the agreement for the processing of personal data for the beneficiaries of the school institution - students and parents. If students are over 16 years old, they can sign the declaration for data processing. In the case of a contract, when the students are still minors, the agreement must be signed by their legal representatives.
The agreement implies the acknowledgment of the provisions of the GDPR and the consent for the processing of the specified personal data, by the institution. In general, the data of students and parents processed in a school are name and surname, citizenship / nationality, home / residence address, personal numerical code, date and

place of birth, series and no. identity card, photo / filming, handwritten signature, e-mail address, telephone number, profession and job, marital status, education and training, school results. The data subjects must express their agreement / disagreement regarding the publication of the name / image / filming on the social / web page of the school, as well as the agreement / disagreement for uploading the data in the electronic catalog.
The school has the obligation to inform the beneficiaries about the purpose of the processing, the duration of the processing (usually corresponding to the period of the educational contract), the persons and institutions that may have access to the stored data, as well as their data protection rights.

2.6. Posting the rules and statements on the school website

Schools that have a website can publish the internal regulations on personal data protection and the specific declarations / agreements, for a better transparency and a complete picture of how the GDPR is applied in the respective unit. It is necessary for all beneficiaries of the educational institution, direct and indirect, to know that the institution collects and processes personal data in accordance with the GDPR.

Figure 2: Steps to applying GDPR in schools
Source: own editing

3. PRACTICE

3.1. Responsibilities of the DPO

The commissioning in practice phase is the most complex as the protection of personal data requires attention every day, not just periodically. The school is an institution that processes personal data daily, so the DPO and the employees of the institution must know very well and apply the provisions of the GDPR to avoid security incidents. At the implementation stage, the data protection officer must periodically train school staff on any new legislation or changes to the rules of procedure. The DPO must keep a register for all external requests to take over data collected by the school. His responsibilities include involvement in all aspects of personal data protection; keeping all access codes and passwords confidential; advising and guiding the director of the institution; responsibility for the guidance

and information provided; permanent monitoring of compliance with the Regulation; cooperation with the National Authority for the Supervision of Personal Data Processing; elaboration of an annual activity report; any other activity deriving from the application of the Regulation.
In order to minimize the risks of security incidents, the DPO may develop certain operational procedures or internal policies, which must be disseminated both in the training of staff and in the online environment, on the school's website.

3.2. Personal data management policy

The educational institution has the obligation to make every effort to ensure the correct management of all personal data collected, regardless of the storage method (catalog, enrollment register, online catalog, SIIIR, etc.). Both the head of the institution and the DPO and employees must process personal data securely, limiting the access of unauthorized persons. Any security incident can have negative consequences for the rights of data subjects, as well as damage to the image of the school. Anyone with access to personal data processed by the school must know, understand and apply the GDPR principles.
There are certain principles of personal data processing, clearly set out in the Regulation: they must be processed transparently, fairly and legally; their processing must be determined by an explicit and legitimate purpose, and may not be further processed for purposes other than those mentioned; the data must be limited to what is necessary in relation to the purpose of the processing, without being processed and unnecessary data, which do not serve the purpose; the data must be real / accurate, and can be updated when necessary; not to be kept longer than necessary or provided by law; be insured against illegal loss / destruction / damage / processing, by taking appropriate organizational or technical measures; be processed in accordance with the human rights of the GDPR; not be transmitted outside the European Economic Area.
Regarding the storage and access to personal data, the school will ensure that the computer system used is secure. Each employee will receive a username and password that will be changed periodically. The computer system will hang if not used for a few minutes. In exceptional cases, personal data may be encrypted or pseudonymized. All storage media will be secured to prevent data theft / degradation / loss. If the data is stored on portable devices, these devices will be password secured, and after the end of the storage period, the data will be permanently deleted. It is recommended to use systems with two identification factors (token, sms, etc.).
The data will be transmitted to third parties (individuals or institutions) only if this is in accordance with the law and the rights of students / parents.
Failure to comply with these procedures regarding the management of personal data may lead to disciplinary sanctions or termination of the employment contract for employees, termination of contracts for employees, taking legal action to recover the image damage caused to the school.

In conclusion

The application of Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data has proven to be a challenge for pre-university education institutions in Romania.

The multitude of personal data collected and processed in a school, the development of information systems and the extent that life in the online environment has gained, lead to a number of difficulties that schools face in implementing GDPR.
Unfortunately, more than a year after the application of the Regulation in Romania, many schools are foreign to its provisions, not yet implementing procedures or policies in this regard. Specialists consider schools to be "safe areas", from which personal information "does not come out". Although, until now, the National Authority for the Supervision of Personal Data Processing has not imposed fines for school institutions, this should not become a general rule for schools to get used to.
In fact, the school must train students as future independent citizens and adaptable to present and future social requirements. The importance of privacy and the protection of personal data are topics that need to be discussed with students from school age, in order to allow them later to make decisions about the personal information to be disclosed, under what conditions and to whom.
As education is based on data, all schools should comply with the GDPR, creating a uniform European legal framework for the protection of data confidentiality of all EU citizens.

References

1. www.edu.ro Ministry of National Education - Protection of personal data, 2018;
2. www.edu.ro Order no. 3844/2016 of May 24, 2016 for the approval of the Regulation on the regime of study documents and school documents managed by pre-university education units, 2016;
3. www.dataprotection.ro General Regulation on data protection, 2018;
4. www.hotnews.ro Pantazi R., Implementation of GDPR in education, 2018;
5. www.republica.ro Grecu E., the GDPR did not reach them. How the Ministry of Education is preparing to change all student cards, 2018;
6. www.24edu.ro School catalog
7. ANSPDCP, Guidance for the application of the General Regulation on Data Protection for operators, 2018;
8. Law no. 102 of May 3, 2005 on the establishment, organization and functioning of the National 9. Authority for the Supervision of Personal Data Processing, with subsequent amendments and completions - Republishing;
10. Law no. 190 of 18 July 2018 on measures for the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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);
11. Law no. 363 of 28 December 2018 on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of preventing,

detecting, investigating, prosecuting and combating crime or the execution of punishments, educational and security measures, and on their free movement date;
12. https://ec.europa.eu/eurostat European Statistics;
13. Guidance on consent under Regulation (EU) 2016/679;
14. Guidance on transparency under Regulation (EU) 2016/679;
15. Security Violation Notification Guide;
16. The guide regarding the right to data portability, reported in art. 20 of the RGDP;
17. The Guide on Data Protection Liability (DPO), reported in art. 37-39 of the RGDP.