COMPLIANCE WITH THE PRINCIPLE OF ACCOUNTABILITY BY THE HIGHER EDUCATION INSTITUTIONS - ADMINISTRATORS OF PERSONAL DATA IN BULGARIA

Radka P. Ivanova[1] and Zhivka Mateeva[2]
[1]Assoc. Prof. PhD., University of Economics Varna, Bulgaria, r.ivanova@ue-varna.bg
[2]Chief. Asst. Prof. PhD., University of Economics Varna, Bulgaria, jivkamateeva@ue-varna.bg

Abstract

Nowadays, the higher education institutions in Bulgaria are facing serious challenges, among which are: the demographic collapse in the country, orientation towards foreign universities - in and outside the EU, high competition between higher education institutions, digitization of the educational process, which in turn lead to a significant increase of the free exchange and access of personal data. One of the most important aspects of the information security of individuals is the protection of personal data. It is part of the right to inviolability and is applied in higher education. In accordance with the current legislation in Bulgaria and in accordance with Regulation 2016/679 (EU), higher education institutions, in their capacity as administrators of personal data, should ensure appropriate levels of data protection. In this regard, the aim of this article is to characterize the higher schools in Bulgaria, with the emphasis being placed on the principle of accountability, appearing as a guarantee for the effective application of the rules for the protection of personal data in the field of higher education.

Keywords: higher school, personal data, personal data controller, principle of accountability, code of conduct

1. INTRODUCTION

The protection of personal data is an important aspect of the information security of the individuals. It is used in various spheres of modern life, including the field of higher education. Bulgarian higher education institutions, in their capacity as administrators of personal data, should ensure appropriate levels of data protection, through the application of adequate technical and organizational measures, as well as make efforts to adapt to new opportunities and challenges based on the development of digital technologies.

According to Art.4, item 7 of the GDPR (General Data Protection Regulation), "administrator" means a natural or legal person, public body, agency or other structure, which alone or together with others determines the purposes and means for the processing of personal data; where the purposes and means of this processing are determined by the Union law or the law of a Member State, the controller or the special criteria for its determination may be established in Union law or in the law of a Member State. The basic rule is that the controller of personal data should comply with the rules for the protection of personal data, complying with the

conditions under which he is entitled to process the personal data. They are related to the basic principles in relation to data quality, including the principle of accountability.

The Higher education is reduced to activities such as teaching, research, social services. It requires the use of personal data for the identification of its participants - teachers, trainees, administrative staff. All of them are in constant interaction with each other and handling of information subject to legal protection. As a specific sector of activity, higher education has its own specifics, which accordingly determine the requirements for its development.

2. ANALYSIS OF THE CHARACTERISTICS OF HIGHER EDUCATION INSTITUTIONS IN BULGARIA FOR THE PERIOD 2017-2022

The Higher education in Bulgaria, according to the Law on Higher Education (LHE), is acquired in higher schools that were established in accordance with the procedure specified in the LHE and received accreditation from the National Agency for Evaluation and Accreditation (NAEA). It is a mandatory requirement that higher education conform to universal human values and national traditions, not depending on religions, ideologies and political doctrines.

According to the Law on Higher Education, higher education institutions are communities of teachers, staff and students who are responsible for achieving the goals of higher education. From a legal point of view, higher education institutions are defined as non-profit legal entities that work for the public benefit and have as their subject of activity the training of specialists with qualifications in a specific professional field; increasing the qualification of specialists; development of science, culture, artistic and sports activities; conducting scientific and applied scientific researches depending on the directions and specialties for which the accreditation has been obtained.

The operation of higher education institutions in Bulgaria is subject to the principle of academic autonomy, which according to the Higher Education Act is expressed in freedom of teaching, research, creativity and dissemination of knowledge; determination of student training majors; election and mandate of academic governing bodies; right to develop internal regulations for organization and management of the activity; free selection and appointment of members of the academic community; the right to build, own and manage the necessary material base for training, research and social services for students, doctoral students, teachers and employees; the right to associate with other organizations and higher schools for joint activities, international cooperation, be subject to contracts and memberships in international organizations; independent determination of the rules for the admission of students, doctoral students and specialists, as well as the fees for training in specialties; independent concluding of contracts for training and upgrading the qualifications of specialists with higher education, for carrying out research (scientific and applied).

The law gives academic freedom as a right to both the main stakeholders who are in constant interaction with each other in higher education institutions, namely – teachers and students. The academic freedom of teachers is reduced to their right to carry out teaching, research and publication activities without being subject to non-scientific sanctions, as well as to have the opportunity for continuous academic development. With regard to students, academic freedom is associated with granting the right to choose their own specialty and university in which to study; to choose the form of study, to be able to evaluate their teachers, to realize academic mobility during the study process in foreign universities of their choice.

The analysis of the data on the number of universities in Bulgaria for the last five academic years shows consistency in quantitative and structural aspects. Their total number is 54, of which 50 are universities and 4 are independent colleges (See Fig.1).

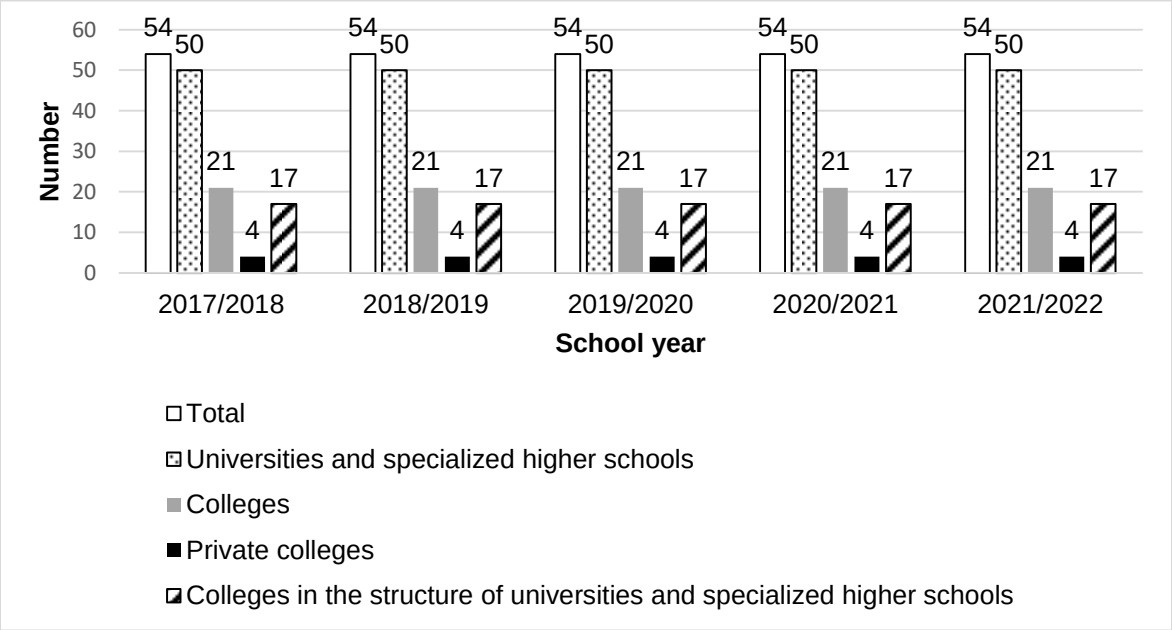

Fig.1. Distribution of higher education institutions in Bulgaria by type for the period 2017-2022

In terms of the number of students being taught, however, a decreasing trend is observed, with 5% fewer in the academic year 2021/22 compared to those in 2017/18 (see Fig. 2).

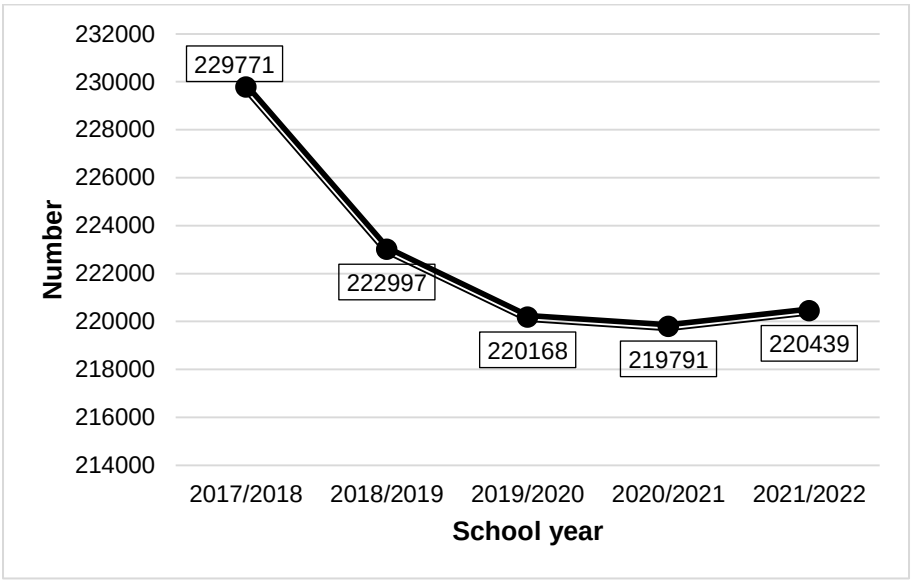

Fig.2. Dynamics of the enrolled students in the three areas of study in higher schools in Bulgaria for the period 2017-2022

A similar trend is observed among the teaching staff in the higher schools in Bulgaria within the period under review. The teachers working in them in the last academic year (2021/22) are 5.6% less than in 2017/18 (see fig.3).

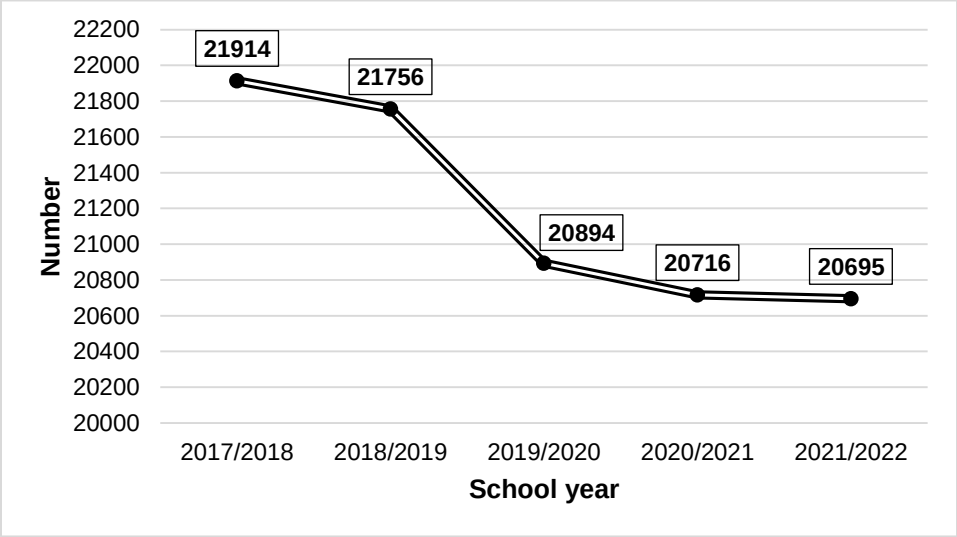

Fig.3. Changes in the number of teachers in higher education institutions in Bulgaria for the period 2017-2022

The students and their teachers in higher education schools become part of them, providing their personal data. This data is used to identify the subjects, in order to uniquely identify them, as well as to grant them access to the resources of the educational institution. The transition to distance learning as a form of effective conduct of the entire educational process due to the COVID-19 pandemic in Bulgaria since March 2020 has further strengthened the attention to protecting the privacy of personal data of students and teachers, as well as the protection of teaching and learning resources. Distance learning platforms were developed, the main issue in connection with which was the limitation of remote access to their resources. Regardless of the observed decreasing trend in the number of both students and teachers during the last five academic years in Bulgaria, one of the main duties of the heads of higher education institutions is to preserve the privacy of their personal data. In this regard, the requirements of the Personal Data Protection Act (PDPA) should be observed. According to it, universities should create a procedure describing the way of collecting, handling and storing information of a personal nature. It is necessary to appoint a special person under the PDPA to monitor compliance with the legal requirements. Higher education institutions in Bulgaria, as administrators of personal data, have the task of applying the principle of accountability, developed in a special regulation by the EU in 2016. The implementation of this implies the use of appropriate tools to assist in the protection of personal data.

3. TOOLS SUPPORTING HIGHER EDUCATION INSTITUTIONS IN APPLYING THE PRINCIPLE OF ACCOUNTABILITY

The principle of accountability is new and is provided for in Art. 5, par. 2 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals in regards to the processing of personal data and on the free movement of such data, briefly referred to below as "GDPR". It is introduced with the reform of the EU data protection rules, on the recommendation of the Work Group under Art.29 of Directive 95/46/EU[1], according to which its inclusion in the new legislative framework will strengthen the role of the administrator and increase his responsibility in the processing of personal data (WP 173, p.8). The principle requires the administrator to comply with all the principles of data protection laid down in Art. 5, par. 1 of the GDPR, namely: lawfulness, good faith and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality. At the same time, the principle requires the controller of personal data to be able to prove the compliance of his activity with these principles at any given time. The legality of the proof in case of possible disputes with the data subjects rests entirely on the administrator (Aleksandrov, 2018, p. 50). This means that administrators should put in place internal mechanisms and efficient measures to

[1]According to Article 29 the Work Group is the independent European work group that operates with matters related to the protection of privacy and personal data until 25 May 2018, i.e. the date of entry of Regulation (EU) 2016/679.

implement the principles, as well as they are obliged to create a documentary trail about the processing. In essence, compliance with the principle is also proof of fulfillment of the obligations of the personal data administrator. In this regard, the traceability of data processing processes in the field of higher education should be carried out through a written document. Specifically, the idea of the principle is that higher education institutions, as administrators of personal data, should eventually acquire the habit of properly documenting all data processing processes in the field of education. In this way, higher education institutions will have greater control and will be able to maintain better data management, as well as in the event of an inspection by the national supervisory authority, they will be able to prove compliance with the GDPR rules.

The accountability principle is implemented through obligations that vary depending on the risk. In order to assist the administrator in implementing the principle of accountability, in the Regulation, are specified various instruments. The most important of them are the following:

A) Keeping Records Of Personal Data Processing Activities

The obligation to keep a register is contained in Art. 30 of the GDPR and is essential for compliance with the principle of accountability. This obligation has been introduced for both administrators and processors of personal data, who should maintain a register of all categories of processing activities carried out on behalf of the controller. Maintaining processing activities is a form of reporting on certain circumstances related to the processing process (Feti, 2018, p. 39).

The registers are maintained in written form, including in electronic format. Depending on whether the register is maintained by an administrator or a personal data processor, the content of the register is explicitly distinguished in Art.30, par.1 and 2 of GDPR. For example, the register maintained by the higher school - personal data controller, should contain at least the following information:

- **Name and Contact Details** – it is necessary to indicate the data of the higher school as data controller, as for all joint administrators. In case where the administrator has designated the data protection officer, his data is also to be indicated in the register;

- **Purpose of Processing** – students' application and admission; provision of educational and other academic services to learners (students, doctoral students and specialists, including candidate students); administration of training and organization of the training process; management of human resources and implementation of financial and accounting efficiency, as well as pension, health and social security activities when processing personal data of workers and employees, etc.;

- **Categories of Data Subjects** – students, doctoral students, specialists, including prospective students, teachers, employees, etc., whose data are processed;

- **Categories of Personal Data** – these may be data regarding physical identity, education, health status, etc., related to the provision of educational services to candidate students, students, doctoral students, specialists and other individuals;

- **Categories of Recipients to Whom The Personal Data Have Been or Will Be Disclosed, Including Recipients In Third Countries or International Organizations** - these may be competent state authorities, which by virtue of a legal act have the authority to require the university to provide information, including personal data, such as the Ministry of Education, Revenue Authorities, Judicial Authorities, etc.;

- **Transmission of Personal Data to A Third Country or International Organization** - such transmission should only take place if there are justification for this and after the individual has been appropriately informed;

- **Data Storage Periods** - the university can store the data of students, doctoral students, specialists who have provided them during their enrollment, for the entire duration of their studies. After their graduation, the data should be archived and stored indefinitely for the purpose of protecting the legitimate interests of the university;

- **Technical and Organizational Security Measures** – they must ensure an appropriate level of security, taking into account the achievements of technical progress, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks posed by the processing with varying probability and legality on the rights and freedoms of the data subjects. Appropriate technical and organizational measures should be taken both at the time of determining the means of processing and at the time of the processing itself,

in order to ensure compliance with the principle of integrity and confidentiality. For this purpose, the higher education institution should adopt internal rules and policies for data protection, which must be well known and observed by both the administrator and his employees, in order to prevent misuse of personal information. For example, data should only be processed by designated persons; the buildings and premises where the data is stored must be secured against burglary, fire, natural disasters; the passwords for access to the data are known only to certain staff members and to be changed regularly, etc. It should also be possible to restore personal data in the event of loss or destruction.

The obligation to maintain a register of personal data processing activities is provided for data controllers/processors that have 250 or more employees. An exception to this obligation is provided by the GDPR in cases where:

- There is a possibility that their processing may pose a risk to the rights and freedoms of data subjects;
- Processing is not sporadic;
- The processing involves special categories of data or personal data related to convictions and offences.

The bookkeeping and the regular updating of the register allows the administrator to make an accurate assessment of the circumstances related to the processing of personal data. Moreover, through the register, the supervisory authority will gain insight into the processing and, in the event of data processing violations, will be able to exercise its powers to protect personal data.

B) Designation of a Data Protection Officer in the Cases Provided for in the Applicable Legislation

The "data protection officer" figure is not new. In Bulgaria, before the adoption of the GDPR, there was a legal possibility to appoint a data protection officer, resulting from the repealed Ordinance No. 1 of 30.01.2013 on the minimum level of technical and organizational measures and the permissible type of personal data protection, and the repealed Directive 95/46/EC did not require organizations to appoint a data protection officer. But in practice, in the last four years since the adoption of the new legal framework for the protection of personal data, the figure of "administrative official" has evolved. The GDPR expressly regulates the designation of such a person, which is mandatory in certain cases. The right choice of a data protection officer can be decisive for the security of the processed data (Aleksandrov, 2021, p. 45). Moreover, the designation of a data protection officer is essential as it will ensure compliance with data protection rules by the controller and also the controller's employees will be informed and be made familiar with the scope of the GDPR and will be trained on the lawful processing of the personal data of individuals.

According to section 4 of the GDPR, the administrative official is an employee of a personal data controller or external to the controller's organization individual charged with advisory functions in the field of personal data protection, supervision of compliance with the GDPR in the controller's organization and raising awareness and training of the staff. The main role of the data protection officer is to ensure that the administrator processes the personal data of its employees, customers, suppliers or other persons in accordance with the applicable data protection rules. The GDPR introduces certain requirements for individuals practicing the profession of data protection officer. The requirements for the appointment of such a person can be conditionally divided into positive and negative.

The positive conditions are specified in Art. 37, paragraph 5 of the GDPR. According to the aforementioned provision, the data protection officer is determined primarily on the basis of his professional qualities and relevant practical skills in the field of data protection legislation. This requirement is linked to the competent performance of the main tasks of the data protection officer. However, the GDPR lacks requirements regarding special education, acquired qualifications, completed training, etc. to occupy the position. Therefore, it is the administrator who assesses whether the person possesses the relevant professional qualities and knowledge necessary to occupy the position. The main role of the official is to familiarize the administrator/processor in detail with the processing of personal data, in relation to the requirements of the GDPR and internal legislation regarding their compliance. In this sense, the official must have a good knowledge of the sector and the organization of the controller in order to be able to determine on what grounds the data is processed by the controller, how long it should be stored, and who should have access to it. In second place is the person's ability

to perform the tasks, specified in Article 39 of the GDPR. The main tasks are: informing and consulting the administrator/processor and employees processing personal data; supervision of GDPR compliance in the administrator's organization; participation in relation to impact on data protection, consisting of giving an opinion when requested by the administrator; cooperation with the supervisory authority. A person's ability should be interpreted in terms of his personal qualities and knowledge such as integrity and high professional ethics (WP 243 rev.01, 2017, p. 12), as well as in relation to his position within the administrator's organization. The negative premise that the GDPR takes into account is the conflict of interests in connection with the other duties and tasks performed by the official in the administrator's organization. In this regard - the provision of Art 38, par. 6 of the GDPR requires the administrator/processor of personal data to do what is necessary so that these tasks and duties do not lead to a conflict of interest. This is because the conflict of interest is an obstacle to the person exercising their functions as a data protection officer. This condition is closely related to the requirement of independence of the official, which means that the controller/processor and all their employees must refrain from giving instructions on the performance of the official's tasks.

According to Art 37, par. 1 of the GDPR, the data protection officer must be determined by the administrator/processor of personal data when:

- The processing is carried out by a public body or structure, with the exception of courts in the performance of their judicial functions;
- The main activities of the controller or processor consist of processing operations which, due to their nature, scope or purposes, require regular and systematic large-scale monitoring of data subjects;
- The core activities of the controller or processor consist of large-scale processing of special categories of data or data related to convictions and offences.

Therefore higher education institutions, as administrators of personal data, should e designate and appoint a data protection officer. As the selection of the administrator during his appointment is the first step in the introduction of GDPR requirements and is essential for compliance with the principle of accountability.

C) Registering of Any Personal Data Security Breach

According to Art 4, item 12 of the GDPR, personal data security breach means a security breach that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data. The violation may eventually cause a number of significant adverse consequences for individuals, which may cause physical, material or non-material damages (WP250, 2017, p. 10). The damage caused by the misuse of personal data in most cases is related to fraudulent credit card transactions, identity theft, mortgage fraud, and more. Therefore, taking appropriate measures by administrators to ensure a higher level of personal data protection is imperative. In this regard, the provision of Art 33 of the GDPR imposes a notification requirement on controllers in certain circumstances in order to limit the impact of data security breaches and to assert the rights of the individuals. According to the aforementioned regulation, when the controller of personal data determines that a breach of data security has occurred, he must notify the competent supervisory authority, unless there is a possibility that the breach will create a risk to the rights and freedoms of the individuals. Notification of the supervisory authority is mandatory for the GDPR administrator and failure to do so will result in the imposition of administrative penalties pursuant Art 83 of the GDPR or corrective measures under Art 58, par. 2 of the GDPR. The administrator may be released from the obligation to notify in case of data security breaches only if he proves that the breach is unlikely to lead to a risk to the rights and freedoms of the affected people.

Depending on the circumstances of the particular breach, the administrator should make a judgment as to whether or not there is a breach of security. However, it will not always be relatively clear to the administrator that a breach has occurred from its very occurrence. In other cases, it may take some time to determine if personal data has been compromised in any way. For example, a higher education data breach would occur in the case of a lost or stolen device containing a copy of a university student, doctoral, graduate, or staff database. It will not be a violation if their data is temporarily unavailable during scheduled maintenance of the database system designed to support and digitize the work activity of the higher school administration. Therefore, the controller's judgment on a case-by-case basis is essential.

The administrator is obliged to document any violation of the security of personal data, including the facts related to the violation of the security of personal data, its consequences and the actions taken to deal with it, according to Art 33, par. 5 of the GDPR. In this sense, the notification of the supervisory authority in the event of data security breaches is an important tool for strengthening compliance with the requirements for the protection of personal data laid down in the GDPR. The purpose of the notification to the supervisory authority is primarily the protection of the individuals and their personal data. In addition, a notice is an important factor in the follow-up of the supervisory authority, in regards to the implementation of its powers granted by the GDPR to implement an effective supervisory mechanism in the field of personal data protection.

D) Adherence to Approved Codes of Conduct or Approved Certification Mechanisms

The Code of Conduct is a new and important tool for compliance with the principle of accountability. It contains a set of internal rules, guidelines and practices that establish ethical standards for controllers/processors of personal data. The legal framework of the code of conduct is contained in Art 40 and 41 of the GDPR. The development and adoption of a code of conduct is not mandatory, but given the rapid technological development leading to a significant increase in the free exchange of personal data, as well as the digitalization and modernization of the educational process, the code will definitely help the effective implementation of the rules for the protection of personal data in the field of higher education. The usefulness of the codes as an accountability tool is that they contribute to the proper application of the GDPR by controllers and processors belonging to a sector or carrying out a similar subject-matter activity, taking into account the specific characteristics of the sector concerned (Toshkova-Nikolova, Feti, 2019, p. 312). In this sense, the code of conduct is suitable for controllers/processors of personal data belonging to the higher education sector, as it will serve as a rulebook for the relevant higher education institutions to adhere to in their data processing activities. Certainly, the adoption of such will contribute to the achievement of the following main goals: providing users of educational services with a tool for assessing the level of personal data protection in higher education institutions in the country; providing higher education institutions, regardless of their size or profile, with methodological guidelines for evaluating and achieving compliance with European and national legislation in the field of personal data; providing higher education institutions with a structured mechanism to demonstrate transparency to supervisors and all other higher education stakeholders (Prodanov, 2021, p. 175-176).

Currently, Bulgaria lacks a code of conduct in the field of higher education. In order to contribute to the proper implementation of GDPR and personal data protection legislation, Member States, supervisory authorities, the European Data Protection Board and the European Commission are obliged to promote the development of codes of conduct. The national supervisory authority for Bulgaria is the Commission for Personal Data Protection (CPDP), which gives an opinion on whether the draft code of conduct, its addition or amendment, complies with the GDPR. In this regard, the CPDP carries out a comprehensive evaluation and review of the draft code of conduct, based on the provisions laid down in Art 40 and 41 of the GDPR requirements, as well as in accordance with the criteria under Art 66 of the Rules of Procedure of the CPDP and its administration. When the commission finds that it provides sufficient adequate guarantees for data protection, it approves it.

Undoubtedly, the adoption of a code of conduct in the field of higher education is a matter of great practical application, as it establishes a uniform standard for the processing of personal data by higher schools. The Code will play a significant role in the correct and effective application of the GDPR, in the fulfillment of the requirements for liability and in the reporting of the specifics of higher schools operations in data processing, as well as will help to comply with the principle of accountability.

4. ACKNOWLEDGEMENT

The higher education is the last level of formal education and takes place in specialized schools (universities and colleges). It has an important role for the development of the economy as a whole, as it can be considered as an economic sector in itself and at the same time - it is a source of a workforce with a higher qualification. Training a large number of individuals implies handling their personal data and accordingly finding ways and means to protect them.

Bearing in mind what has been said so far, we can summarize that with the adoption of the GDPR, the rules for the protection of personal data have been updated, through the introduction of the new principle of accountability, which helps to strengthen the level of protection in all areas of modern society, including in higher

education. The principle requires detailed planning and documentation of processing activities, which stimulates the responsible attitude of controllers towards data protection. In this sense, accurate and precise compliance with the principle of accountability is a key element to guarantee respect for the rights of data subjects. At the same time, its correct application will lead to an end to the practice of absolutely uncontrollable collection and use of data and will create conditions for quality processing of personal data.

REFERENCE LIST

Aleksandrov, A. (2021). Dlazhnostno litse po zashtita na dannite – iziskvaniya, status i funktsii. Zashtitata na lichnite danni i digitalizatsiyata – predizvikatelstva i perspektivi. Nauka i ikonomika, s. 44-55

Aleksandrov, A. (2018). Ot 25 may 2018 godina zapochva da se prilaga Obshtiyat reglament za zashtita na lichnite danni. Trud i pravo, br. 4, s. 44-51

Feti, N. (2018). Poddarzhane na registar na deynostite po obrabotvane na lichni danni. Trud i pravo, br. 9, s. 37-48

Prodanov, G. (2021). Kodeks za povedenie vav vrazka s obrabotvaneto na lichni danni v sferata na vissheto obrazovanie. Zashtitata na lichnite danni i digitalizatsiyata – predizvikatelstva i perspektivi. Nauka i ikonomika, s. 172-179

Toshkova-Nikolova, D., Feti, N. (2019). Zashtita na lichnite danni, Sofiya: IK „Trud i pravo“

WP 173 (2010). Article 29 Data Protection working party. Opinion 3/2010 on the principle of accountability. Adopted on 13 July 2010

WP 243 (2016). rev. 01, Article 29 Data Protection working party. Guidelines on Data Protection Officers (“DPOs”). Adopted on 13 December 2016, As last Revised and Adopted on 5 April 2017

WP 250 (2018). rev. 01, Article 29 Data Protection working party. Guidelines on Personal data breach notification under Regulation 2016/679. Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018

https://nsi.bg