Audit 2 (2020), Cild 28, səh. 95-104.
Audit 2 (2020), Vol. 28, pp. 95-104.

Zhivka Mateeva Stoyanova , Ch. Assist. Prof., Ph.D.
University of Economics – Varna
Address: Boul. "Knyaz Boris I" 77, Varna, 9002, Bulgaria
E-mail: jivkamateeva@ue-varna.bg

UDC 342.721
JEL K-36, K-38

PRINCIPLES OF PERSONAL DATA PROTECTION

Abstract

The topic about the personal data protection principles and the protection of the natural person's data based on these principles is of great interest for both theory and practice. The article explores the application of the personal data protection principles. A focus is laid on the current and modernized basics for data protection as guarantee for better control and security of the natural person's data in the modern digital world. Based on analysis of these principles, the focal points of their application are established. This is the basis which outlines the practicality of the principles related to regulating personal data collection, storage and processing.

Keywords: principles, personal data, lawfulness, transparency, accuracy, confidentiality, accountability.

Introduction

Personal data protection principles have been acquiring ever greater public significance and acknowledgement over the recent years, as there is almost no sphere in the contemporary social, economic, public and political life which does not require the performing of activities relating to the processing and use of personal data, as well as acquiring access to such data. All that, undoubtedly, creates specific personal data protection problems linked to the danger and hazards from unfavourable consequences for the natural person. In this regard, in 2016 a new legal framework was introduced in the EU in the sphere of personal data protection, including Regulation (EC) 2016/679 of the European Parliament and the Council of 27 April 2016 concerning the protection of natural persons with regard to personal data processing and the freedom of movement of such data.

As part of the reform pack for data protection, the Regulation superseded Directive

Audit 2 (2020), Cild 28, səh. 95-104.
Audit 2 (2020), Vol. 28, pp. 95-104.

95/46/EC[1] and has been applied directly by the EU member states as of 25 May 2018. It introduces a serious advancement in the right of natural persons concerning personal data as compared to the framework existing before. It aims at guaranteeing consistent and uniform application in the Union of the regulations for protection of the basic rights and freedoms of natural persons with regard to personal data processing.

Personal data processing is a globalised process requiring the introduction and development of universal principles of natural persons with regard to their personal data processing.

Until the introduction of the Regulation, personal data protection principles were internationally recognized in Convention №108[2] and Directive 95/46/EC, as well as in the national legislation – more specifically the Law on Personal Data Protection. The main difference there was in the normative support of the principles. While in the Convention they were elaborated in a separate chapter and in the Directive in separate provisions, the Bulgarian legislator had them elaborated as rights and obligations of the legal entities [6, p. 234-237]. This inexorably leads to decreased effectiveness in the application of the basics of inviolability of the person and personal life of natural persons. Undoubtedly, the adoption of a whole new regulation in the sphere of personal data protection leads to furthering and upgrading the already existing rules and regulations as well as achieving harmonisation of the regulation all through the EU without the need to have it officially transposed in the national legislation. Despite the fact that the Regulation does not arise from radically differing principles in the legislation which it introduces, it was necessary to systematise their range and manifestation within a consistent and integral legal framework which helped countermand the existing difference in the amount of protection guaranteed.

The need to clarify the principles within the Regulation is determined, on the one han, by the recent significant changes in the already existing legal framework, and on the other, by the complexity of the process of transposing the new regulations, the manifestation of the significance of the principles in their different aspects, their ambiguous interpreting and construing, as well as the need to have them serve as a benchmark for interpreting and construing by the controllers and the legal authorities.

The goal of the article is to highlight and analyse the content of the principles in the Regulation in view of the new legislative changes guaranteeing the observance of the personal data protection rules through the full readiness of their implementation by the administrators when processing personal data.

[1]Directive 95/46/EC of the European Parliament and Council of 24/10/1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OBL 281, 23/11/1995, p. 31-50.

[2]Convention 108 of the Council of Europe of 28/01/1981 on the Protection of Individuals with regard to Automatic Processing of Personal Data was modernized in May 2018. Currently the Report on its amendment is signed by 30 states, among which the Republic of Bulgaria, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures (10/06/2019).

Audit 2 (2020), Cild 28, səh. 95-104.
Audit 2 (2020), Vol. 28, pp. 95-104.

Exposé

The principles of personal data protection apply to all controllers and concern any and all acts of data processing, because of which knowing them well is not an end in itself. Their main purpose is to maintain relevant control over non-public data which refer to the identifying of a certain physical person. They have special significance as they are the basis for a correct interpreting and application of the Regulation, as well as guidelines for controllers when processing personal data. Because of that the key to the observance of the applicable law is to abide by the following seven principles of data quality.

Principle of lawfulness, fairness and transparency

The first principle set out in Article 5, para. 1, (a) of the Regulation requires that personal data be processed lawfully, fairly and in a transparent manner. That generally means controllers must in the first place have legal grounds for processing personal data and secondly, never use such data in a manner which may have unjustified consequences for the persons concerned and thirdly, submit information on the legal grounds for the data processing.

Data processing is lawful when personal data controllers have legal grounds for the data processing. Because of that and in view of the principle of accountability, data controllers need to process such data on the grounds of the following legal requirements stipulated in Article 6 of the Regulation:

a) when there is consent by the natural person;

b) performance of contractual agreements to which the data subject is party;

c) for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject;

e) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;

f) for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

At least one of these conditions needs to be applied whenever personal data are processed. For instance, the information related to performing educational and other academic services for university students, PhD or postgraduate students collected via the application forms and enrolment papers for the establishment is processed rigidly on the legal grounds provided by a special law which is applicable in this case. The personal data the higher educational establishment is authorised to collect and store are explicitly stipulated in the Higher Education Law, the Ordinance on State Requirements for Enrolment of Students in Higher Educational Establishments in the Republic of Bulgaria. It is this special legislation which determines the admissibility and amount of the collected and stored data, because of which the processing of personal data of college and university students is also lawful as a rule. When assessing the lawfulness of data processing in this case, it is of great importance to observe not only the applicable law on personal data protection but the mandatory provisions of the special laws as well.

Fairness means particular behaviour of the controller concerning the data subject which

Audit 2 (2020), Cild 28, səh. 95-104.
Audit 2 (2020), Vol. 28, pp. 95-104.

must be adequate and not excessive in relation to the purpose and is not contrary to accepted principles of morality[3] . The importance here is on the fact that this element of the principle requires from the controller to process the data fairly and openly, as well as give the data subject enough information about the performance of the processing activities and their purpose. The earliest stage of the realization of the right of the subject to be informed is the time of data collection. Fairness is important mostly in situations in which the data subjects have the right of choice whether to enter into a relation with the controller. If the data subjects are acquainted from the very beginning with the purpose of the data collection, they will be able to decide whether to enter in this relation[4] or not, as well as the chance to prevent eventual misuse of this information or avoid future damage.

Transparency is the third element of this principle. Unlike Directive 95/46/EC and Convention 108, it has been formulated explicitly for the first time in the Regulation and upgrades the fairness principle. Transparency is guaranteed with the data subject‘s right to information, as well as with the data controller‘s duty to provide information. In this respect, data subjects need to be informed in a clear, unambiguous and easy to understand and accurate manner of the processing of their data. The controller should also individualise himself to the data subject, inform him about the processing operations of his personal data, about the grounds and purpose of this data processing, the rights he has in regard to the protection of his personal data and the ways they are exercised. It is imperative that the information given by the controller to the data subject be publicised (on the controller‘s internet page, for instance) and easily accessible, without that requiring too much effort. In this respect, the information cannot be hidden in general agreement conditions and/or inviolability declaration. This is especially relevant for the internet medium where, quite often, the announcements concerning data protection are unclear, difficult to access, not transparent and not always in full compliance with the applicable rules. We can take as an example the behavioural advertisements on the internet where both the increased number participants in the provision of behavioural advertisements and the technological complexity of this practice do not allow the data subject to realise or know whether personal data are collected, by whom and for what purpose. As for behavioural advertisement, data subjects have to be informed about the identity of the provider of the network broadcasting the advertisement and the purpose of the data processing. The Data subject has to be clearly informed that the cookie[5] will allow the advertisement provider to collect information about the visits to other websites, about the advertisements shown, about those of them which have been activated, the time of viewing, etc.

[3] Unfair processing of personal data exists if the controller misuses his dominant position regarding the data subject in order to obtain his consent to process his personal data.

[4] For more on the nature of the relation see [4, p. 22-26].

[5] A cookie is a small text file containing letters and digits which is stored in the data subject's computer and is later used by the network provider. This text can have different functions, e.g. storing information about preferences, about the sessions or for identifying the subject via a unique identification code. In the context of behavioural advertising, a cookie allows the provider of the network which also provides advertising to recognise someone who had visited the site before, who visits the site again or visits another website which is a partner to the advertising network [10, p.7].

Audit 2 (2020), Cild 28, səh. 95-104.
Audit 2 (2020), Vol. 28, pp. 95-104.

Principle of purpose limitation

The second principle set out in Article 5, para. 1, (b) of the Regulation requires that personal data be collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This principle supposes that the purpose for which the data are collected should be clearly defined before the process of collection begins. This shall limit and prevent any uncontrolled data processing.

The purpose of the processing must be legitimate, not incompatible with the Regulation and must be clearly defined by the controller who stores the data. Practically, the controller must define beforehand clearly and explicitly the purpose for which he needs to process such personal data. Personal data can be collected and processed only for the purpose stated. Because of that, the processing shall be deemed inadmissible if the controller violates that purpose. Any new purpose different from the one initially stated means further processing. For instance, placing fast loan advertisements in the envelope together with the bills of the subscriber means further processing, since the controller processes further his subscribers' data for direct marketing purposes. In this case, this means further processing which is incompatible with the purpose for which the data have been initially collected. Because of that the collector is obliged[6] to inform the data subject and receive their consent or process the data on other legal grounds.

The further processing will be permissible only if there is compatibility between the initial and the further purpose for which the data are used. In this case, no separate legal grounds are required differing from the ones for which the collecting of personal data was initially permitted.

No assessment of compatibility of purposes is required when the further processing of the data is for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, as it is considered not to be incompatible with the initial purposes, as provided in Article 89, (1) of the Regulation, subject to implementation of guarantees by the controller in order to safeguard the rights and freedoms of the data subject [7, p.94].

Such guarantees are given through the implemented technical and organisational measures, which retain the processed information to the bare necessary minimum.

Principle of data minimisation

This principle, set out in Article 5, para. 1, (c) of the Regulation, requires the processing of personal data limited only to what is absolutely necessary for the purposes for which they are processed. The controller has the duty to process personal data only when such processing is adequate and appropriate. Also he is only free to process those data which are relevant and crucial for achieving the purpose and without which its realisation is not possible.

In order to keep this principle, it is necessary to assess the need of processing personal data, as well as determine the minimum amount of data compatible with and proportionate to the purpose at hand.

[6] Such obligation to inform data subjects would increase the transparency of further processing and improve the exercising of the rights of the subjects with regard to other processing operations [9, c. 8].

Audit 2 (2020), Cild 28, səh. 95-104.
Audit 2 (2020), Vol. 28, pp. 95-104.

Any data collection above the appointed minimum is excessive and unproportionate. For instance, when a natural person applies for a bank loan, the bank collects data about him in order to make sure that person will be able to pay regularly the loan deposits. Collecting any other information which does not bear relevance with this purpose (health, ethnicity, etc.) is unjustified and the bank has no right to require it. The data stored by the controller should not include irrelevant details. What is more, the bank does not need to now certain personal information which appears as excessive and unproportionate, especially in the cases when the purpose can be achieved without it.

Another infringement of that principle is collecting additional information about the natural person with the idea that it may be used for future purposes. It is inadmissible to collect and store personal data –just in case. Even in the event that the data subject has given his explicit consent, there are no legal grounds for such processing.

Principle of Accuracy

The provision of this principle as set out in Article 5, para. 1, (d) of the Regulation requires accuracy of personal data, and where necessary be kept up to date. In this sense the controller needs to check the reliability of the source of the information.

It is the controller's responsibility to observe this principle, but this does not always depend on his behaviour as much as it does on the conscientiousness of the data subject. It is recommended that the controller inform the natural persons about the necessity of their timely cooperation for updating their personal data whenever there is a change in them.

There is no infringement of this principle if the information is accurately recorded and provided by the data subject, as well as when reasonable steps are taken to guarantee the veracity of the information. In order to avoid any risk of causing damage to natural persons, data controllers need to take all reasonable steps to timely erase or rectify any inaccurate or plainly wrong personal data and also take the purpose for their processing into consideration. E.g., if the data are used for making decisions which may significantly influence the natural person, then every effort must be made to guarantee the accuracy (e.g., processing of inaccurate medical information about a patient may lead to a high risk to his health). If necessary, the data must be kept up to date, which will guarantee their accuracy.

Principle of storage limitation

The provisions set out in Article 5, para. 1, (e) of the Regulation, stipulate that personal data be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Storing personal data for too long, as a processing operation, can lead to serious problems, such as breach of the data subject's privacy, of his personal data and other of his rights, freedoms, and vital interests. For that reason exactly, the principle stipulates that personal data should be stored for a limited period of time only. This period can be regulated by the authorities or by the controller. In the first case, the controller is obliged to store the data for the period determined in the regulation. In Poland for instance, the employer is obliged to store the employee's work file for up to 50 years after the termination of the employment agreement [8, c. 16]. While in Bulgaria, and more specifically the Labour Code, does not provide period limits for the storage of the different types of documents, part of the

Audit 2 (2020), Cild 28, səh. 95-104.
Audit 2 (2020), Vol. 28, pp. 95-104.

employee's work file. Such terms are specified in the provisions of the different laws, depending on the type of document and the information which it contains. Article 12, para. 1, of the Law on Accounting, for example, stipulates the pay statement record books must be stored for a period of 50 years, as of January 1 of the accounting period following the accounting period which the books relate to. In this respect, the processing of the data within the regulated period of time will be deemed legitimate and compatible with this principle.

When there is no appointed period for storing the data in the special laws, the data controller must appoint such a period himself, based on the purpose for which the data was collected. It is important that the controller substantiate the eventual reasonable period of time required for the achievement of the purpose for which the data are stored. The controller cannot store the personal data of participants in procedures for recruitment and selection of personnel for indefinite period of time or one which is too long. In this respect, the principle must be observed in the light of the initiation, realisation and completion of personnel selection procedures in a way which does not impair the realisation of the data processing purpose [12]. The Regulation does not explicitly define the period. But the amendments of the Law on Personal Data Protection of 26/02/2019[7] 1redefined some special cases[8] concerning data processing, including personnel selection procedures. In accordance with the provisions of Article 25к, para. 1 of the on Personal Data Protection, the employer or the employment authority, in their capacity as personal data controller, have to determine a period of time for storing the personal data, which can be no longer than 6 months, unless the applicant has given his consent on a longer period. In order to determine exactly the moment when the period starts, the controller also needs to take into consideration the period of protection of legal claims arising from the selection process. Therefore, the period for storage of the personal data of the participants in personnel selection procedures, as per Article 25к of the Law on Personal Data Protection starts the moment the procedures referred to end, respectively after the expiry of the term for their appealing. There is an exception to that rule when the applicant has given his consent his personal data to be used for the purposes of future recruitment and selection procedures. The legality to have the 6-month period extended depends on the will of the data subject, since he is the only one who has the right at all times and without explanation to withdraw his consent, as a result of which any further processing of the data is terminated.

After the expiry of the period for storing the personal data, the controller must erase or destroy them. One of the most significant changes introduced by the Regulation concerning citizen rights is the right to data erasure, or the right to be forgotten. This is not a new right; before, it was set out in the repealed Directive 95/46/EC, but is further developed in Article 17 of the Regulation. It allows the erasure of personal data when the data subject does not give consent for their further processing or when there are no legal grounds for their being stored [13, p. 9]. Erasure of data can be requested if they are no longer necessary for the

[7] As amended, ST, issue 17 of 26 February 2019.

[8] The largest number of special rules is provided for personal data processing in the context of employment and official relations. This is no surprise, as the Regulation has preserved the opportunity, also provided in the existing legislation on personal data protection, to allow deviations from the general rules when processing of personal data of personnel is at hand [2, c. 50]. For more on the employer's obligations concerning personal data in employment relations, see [1, c. 133-143].

Audit 2 (2020), Cild 28, səh. 95-104.
Audit 2 (2020), Vol. 28, pp. 95-104.

realisation of the tasks of the controller who stored them. For instance, after paying off a loan, the file with the subject's data must be destroyed by the bank-controller of his personal data.

Personal data can be stored for longer periods only for archiving purposes in the public interest, for scientific or historical research purposes, if all appropriate technical or organisational measures have been taken so that the rights and freedoms of natural persons are guaranteed. Such measures can include techniques like data pseudonymisation or anonymisation whose application can lower the risks to the data subject and help data controllers to fulfil their obligations in relation to data protection.

In order to guarantee the observance of this principle, the controller needs to check periodically the necessity for continued data storage. The purpose of these checks is to determine whether the legal grounds for storing the already collected data by the controller are up-to-date and applicable, whether the need for processing these different categories of data still exists, as well as whether the purposes for which the data are collected have not been achieved before the expiry of the stipulated period for storing the data.

Principle of integrity and confidentiality

The sixth principle set out in Article 5, para. 1, (f) of the Regulations introduces the controller's obligation to process personal data in a way which guarantees an appropriate level of security. It is important to note that this principle refers to security in all aspects of personal data processing and aims at preventing the arising of unfavourable consequences from unauthorised or illegal processing, accidental loss, destruction or damage to the data.

This is a new principle proclaimed with the Regulation, even though the requirements for guaranteeing protection against unauthorised or illegal processing or accidental loss, destruction or damage by applying appropriate technical or organisational measures has been provided in the already existing legislation [3, c. 49-50].

Breaches in information security can lead to real damages for the natural person. Such damages in most cases include identity theft, false credit card transactions, mortgage fraud, etc. Because of his, the need and interest on the part of data controllers to take effective measures for guaranteeing real data security grows exponentially. The Regulation does not contain an extensive list of appropriate measures, but only guidelines for possible ones. Therefore, the assessment of which measures are appropriate to apply in each and every case is entirely the controller's obligation.

When determining what measures will be appropriate in any particular case, the controller has to assess all risks relating to data processing. In this respect, it is necessary to take into consideration technical advancements, the cost for applying the measures, the nature of the data, the scope and purpose of the processing, as well as the risks to the rights and freedoms of the natural person. Based on the risk assessment, the controller needs to introduce real and efficient internal protection mechanisms in order to guarantee data security. For instance, the data should be processed only by authorised personnel for this purpose exactly; the buildings and rooms where the data are stored have to be fire and break-in proof and protected against force majeure; the passwords for access to the data need to be known only to the authorised personnel and be changed regularly, as well as measures must be taken to guarantee the restoring of damaged or destroyed data.

Audit 2 (2020), Cild 28, səh. 95-104.
Audit 2 (2020), Vol. 28, pp. 95-104.

Principle of accountability

The seventh principle set out чл. 5, para. 2 of the Regulation requires that the controller observe all the principles set out in Article 5, para. 1, and be able to demonstrate compliance with them. This principle is new and introduced with the reformed rules of the EC for data protection, as recommended by the Working Party per Article 29 of Directive 95/46/EC [9] . According to the Working Party, its inclusion in the new legislative framework will strengthen the controller's role and increase his responsibility in the processing of personal data [11, p.8].

This principle is realised through obligations which vary according to the risk. In view of enhancing the controller's activities towards applying the principle of accountability, the Regulation points a number of instruments, such as: keeping of a register bout the personal data processing activities[10]; all the relations between the controller and the data processor; appointing an official directly responsible for personal data protection complying with the provisions of the law; documenting every breach of personal data security; observing all the approved codes of behaviour or approved certification mechanisms, etc.

Conclusion

In view of the above, we can recapitulate that the adoption of the new legal framework for personal data protection in the EU modernised the principles via the introduction of new requirements for transparency, access and erasure, and accountability, which helps increase the level of protection in all the spheres of modern society. In this respect, the punctual observance of the personal data protection principles is the key element for guaranteeing the safeguarding of personal rights. Moreover, their appropriate implementation will stop the practice of the absolutely uncontrollable collecting and use of such data and create conditions for quality personal data processing.

In order to raise the level of security, it is necessary that not only data controllers know the principles well, but also all the participants in the data protection procedures, so that they can be effectively applied. Knowing them well is not an end in itself, since the principles can be used for assessment of breaches in data processing as well as for determining whether there has been a breach in the natural person's rights. The principles of personal data protection define the boundaries of application of the legislative framework by regulating the collection, the processing of personal data as well as serving as a basis for construing cases of dispute between competing rights. They can help avoid all the limitations of transborder data flow between the EU member states with different standards, as well as decrease the risk of abuse with personal data.

[9] The Working Party as per Article 29 is an independent European working party dealing with issues related to the inviolability of privacy and personal data up until 25 May 2018, i.e. the date of coming into force of Regulation (EC) 2016/679.

[10] An analogous principle is set out in the e-registers for sick leave cards in view of the effectiveness of the specified procedure for introducing or storing of data under basic conditions for accountancy and control and a main goal – not allowing abuse of an any security means, see [5, p. 55-61].

Audit 2 (2020), Cild 28, səh. 95-104.
Audit 2 (2020), Vol. 28, pp. 95-104.

References

1. Andreeva, A. (2018). The Employer's Obligation to Protect Personal Data Collected under an Employment Relationship. International Journal of Economic Research : Serials Publications Pvt. Ltd., 15, 1, p. 133 - 143
2. Aleksandrov, A. (2018). Kakvo predvizhda proektat za izmenenie na Zakona za zashtita na lichnite danni. Trud i pravo, 5(18), p. 46-53
3. Aleksandrov, A. (2018). Ot 25 may 2018 godina zapochva da se prilaga Obshtiyat reglament za zashtita na lichnite danni. Trud i pravo, 4(18), p. 44-51
4. Bachvarova, M., Andreeva, A., Yolova, G., Dimitrova, D., Mateeva, Zh. (2019). Osnovi na pravoto. Varna: Nauka i ikonomika, pp. 378
5. Yolova, G. (2018). Electronic Register of the Medical Certificates Specifics and Functions Related to the Prevention of Abuse in the Health Insurance System.Globalization, the State and the Individual: International Scientific Journal, Varna: VFU Chernorizets Hrabar, 2(18), p. 55 – 61
6. Kiskinov, V. (2005). Balgarsko i evropeysko informatsionno pravo: sravnitelen analiz. Siela, tom 1, pp. 327
7. Toshkova-Nikolova, D., N. Feti. (2019). Zashtita na lichnite danni. Prilozhen komentar, razyasneniya i prakticheski resheniya po novata pravna uredba. S., IK „Trud i pravo, pp. 751
8. Zashtita na neprikosnovenostta na rabotnoto myasto, Narachnik za sluzhiteli, dostapen na adres chrez sayta na KZLD: https://www.cpdp.bg/?p=element&aid=837
9. Proekt na protokol otnosno: 3376-o zasedanie na Saveta na Evropeyskiya sayuz (Pravosadie i vatreshni raboti), provedeno v Bryuksel na 12 i 13 mart 2015 g., 7166/15 ADD 1, Bryuksel, 14 april 2015 g., dostapen na adres:
https://www.parliament.bg/pub/ECD/184858ST07166-AD01.BG15.PDF
10. Opinion 2/2010 on online behavioural advertising (WP 171), Adopted on 22 June 2010.
11. Opinion 3/2010 on the principle of accountability (WP 173), Adopted on 13 July 2010.
12. Stanovishte na Komisiyata za zashtita na lichnite danni reg. № НДМСПО-01-142/14.03.2019 г.
13. Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and The Committee of the Regions –A comprehensive approach on personal data protection in the European Union, COM/2010/0609 final, 4.11.2010.

Məqalə redaksiyaya daxil olmuşdur: 05.03.2020
Təkrar işləməyə göndərilmişdir: 17.03.2020
Çapa qəbul olunmuşdur: 02.04.2020

Дата поступления статьи в редакцию: 05.03.2020
Отправлено на повторную обработку: 17.03.2020
Принято к печати: 02.04.2020

The date of the admission of the article to the editorial office : 05.03.2020
Send for reprocessing: 17.03.2020
Accepted for publication: 02.04.2020