IX INTERNATIONAL SCIENTIFIC PROFESSIONAL CONFERENCE SECURITY AND CRISIS MANAGEMENT – THEORY AND PRACTICE (SeCMan) - IX INTERNATIONAL FORUM „SAFETY FOR THE FUTURE 2023" - 29th and 30th September 2023, Belgrade, Republic of Serbia

PERSONAL DATA PROTECTION – FRAMEWORKS, PRACTICAL EXPERIENCES AND CHALLENGES

Radoslav Rakovic[1a]

[1] Energoprojekt Entel plc, Belgrade, Bulevar Mihajla Pupina 12, Belgrade, Republic of Serbia, rrakovic@ep-entel.com

Received: 25th June 2023
Accepted: 7th August 2023

Review paper

Abstract: *Fundamental information security management standard ISO 27001 declares need for protecting basic features of information – confidentiality, integrity and availability - and defines certain number of controls oriented to technical, organizational and combined actions that should enable it. Particular issue represents personal data protection that is subject of particular General Data Protection Regulation (GDPR) has been appplied in EU from 25.05.2018. and paricular Law on personal data protection of Republic of Serbia has been applied from 22.08.2019. After brief review of the GDPR and the subject law, practical experiences and challenges in application of personal data protection in Serbia are considered.*

Key words: *information security, personal data protection, general data protection Regulative (GDPR), law on personal data protection (LPDP)*

1. INTRODUCTION

The rapid development of modern technologies makes our lives significantly easier, but on the other hand, it brings us problems that we have not had before, or at least we have not had them on that scale. One of the most current problems we face in this sense is information security (ISec). The field of information security, as an approach to preserving its basic properties, is generally regulated by the basic standard ISO 27001 within the ISO 27000 series (ISO 2018, 2022a, 2022b). The basic properties of information - CIA - include *Confidentiality*, that the information is available only to those who have the right to it, *Integrity*, that the information is complete and protected from unauthorized changes, and *Availability*, that the information is available when we need it, provided that we have the right to it.

The specificity of the ISO 27001 standard in relation to other management standards is reflected in the special Annex A, which, according to the latest revision of the standard from 2022 (ISO 2022a), contains 93 controls grouped into 4 categories - organizational controls (chapter 5 - 37 controls), people controls (chapter 6 - 8 controls), physical controls (chapter 7 – 14 controls) and technological controls (chapter 8 - 34 controls). In comparison with the previous revision of standard (114 controls), 11 controls are new and others are renamed, modified or merged.

[a] ORCID: 0000-0002-8067-6582

Protection of personal data represents a very significant and delicate segment of the overall concept of information security. The significance arises from the fact that personal data are present in databases within information systems of various purposes - systems of state bodies (about citizens or taxpayers), banking systems (about bank clients), systems of educational institutions (about pupils, their parents, students, teaching staff), systems in healthcare institutions (about patients, staff, etc.). The delicacy is a consequence of the fact that personal data is closely related to the spheres of our lives that we do not want to share with a large number of people. At the same time, the disposal of that data opens up enormous opportunities for misuse and can have inestimable consequences for our lives.

The protection of personal data is closely related to the universal right to respect for private life, which, together with the rights to respect for family life, the right to respect for home and the right to respect for correspondence, was proclaimed by the UN Universal Declaration of Human Rights from 1948 (UN, 1948). The development of information technologies, the Internet and the information society over time led to the recognition of the need to protect personal data and it was recognized in the European Charter of Fundamental Rights, adopted in 2000 (EU, 2000), where in Art. 8 declares that "everyone has the right to protection of personal data" which must be processed in a fair way, in accordance with the purpose and with the consent of the person.

In this paper, the topic of personal data protection is considered from several points of view. Firstly, the representation of the topic in standards related to information security was reviewed. Then the key documents related to international legal regulations were discussed, i.e. General Data Protection Regulation - GDPR (EU, 2016a) and the Directive considering the application of the GDPR in the field of personal data of persons connected with the investigation of criminal offenses (EU, 2016b). Particular attention was paid to the Law on the Protection of Personal Data in the Republic of Serbia (OGRS, 2018) and the experiences and challenges of its application both at the level of the Republic of Serbia and within organizations.

2. PERSONAL DATA PROTECTION IN STANDARDS AND REGULATIONS

This chapter provides a concise overview of the ISO/IEC 27001 standard, European regulations and laws in the Republic of Serbia from the point of view of personal data protection, and then challenges and dilemmas in their application in practice are discussed.

2.1. Standard ISO/IEC 27001

The significance of personal data protection is already visible from the change in the title of the standard (ISO 2022a) which, in addition to information security includes cyber security and privacy protection. Of course, this topic is also present within controls from Annex A in several places, predominantly in organizational and people controls, Table 1:

- Explicitly, in control A.5.34, which refers to the privacy and protection of personally identifiable information (PII).

- Discussing the security related to human resources before (A.6.1 and A.6.2), during (A.6.3 and A.6.4) and after termination of engagement (A.6.5).

- Defining access rights, including authentication and authorization (A.5.17, A.5.18 and A.8.5).

- Discussing the management of incidents related to information security, including personal data breaches (A.25 to A.29).

Table 1: Controls in Annex a of ISO/IEC 27001:2022 related to personal data protection

Part	Title
A.5	Organizational controls
A.5.9	Inventory of information and other associated assets
A.5.10	Acceptable use of information and other associated assets
A.5.17	Authentication information
A.5.18	Access rights
A.5.25	Assessment and decision on information security events
A.5.26	Response to information security incidents
A.5.27	Learning from information security incidents
A.5.28	Collection of evidence
A.5.29	Information security during disruption
A.5.34	Privacy and protection of personal identifiable information (PII)
A.6	People controls
A.6.1	Screening
A.6.2	Terms and conditions of employment
A.6.3	Information security awareness, education and training
A.6.4	Disciplinary process
A.6.5	Responsibilities after termination or change of employment
A.6.8	Information security event reporting
A.8	Technological controls
A.8.5	Secure authentication

2.2. General Data Protection Regulation (GDPR)

The General Data Protection Regulation 2016/679 - GDPR, (EU, 2016a) was adopted by the European Parliament and the Council on April 27, 2016, and was published in the Official Journal of the European Union (OJEU) on May 4, 2016 and it began to be applied on May 25, 2018. The period of two years from the adoption to the application of the regulation brought many doubts about its content and the possibility of its application, which are still present today. The regulation itself has a total of 88 pages, the first 31 of which contain a preamble with 173 items, which explains the basic elements contained in the regulation. Paragraph (7) of the Preamble, which states that "natural persons should have control over their personal data", should be especially emphasized, and this can be considered an essential reason for adopting the regulation. The regulation itself is presented on the remaining 57 pages, it contains a total of 99 articles that are grouped into 11 chapters, some of which have sections. A summary of the structure of this regulation is given in Table 2 by chapter and section (where they exist). In the table in question, numbers in parentheses indicate articles of regulation that refer to individual segments.

Table 2: Regulative 2016/679 (GDPR) structure

Part	Title
I	General provisions (1-4)
II	Principles (5-11)
III	Rights of the data subjects (12-23)
1	*Transparency and modalities (12)*
2	*Information and access to personal data (13-15)*
3	*Rectification and erasure (16-20)*
4	*Right to object and automated individual decision-making (21-22)*
5	*Restrictions (23)*

Part	Title
IV	Controller and processor (24-43)
1	*General obligations (24-31)*
2	*Security of personal data (32-34)*
3	*Data protection impact assessment and prior consultation (35-36)*
4	*Data protection officer (37-39)*
5	*Codes of conduct and certification (40-43)*
V	Transfers of personal data to third countries or international organizations (44-50)
VI	Independent supervisory authorities (51-59)
1	*Independent status (51-54)*
2	*Competence, tasks and powers (55-59)*
VII	Cooperation and consistency (60-76)
1	*Cooperation (60-62)*
2	*Consistency (63-67)*
3	*European data protection board (68-76)*
VIII	Remedies, liability and penalties (77-84)
IX	Provisions relating to specific processing situations (85-91)
X	Delegated acts and implementing acts (92-93)
XI	Final provisions (94-99)

It is important to note that alongside this regulation, directive 2016/680 (EU, 2016b) was adopted, which limits the application of the GDPR in cases related to the processing of personal data by competent authorities for the purposes of preventing, investigating, detecting and prosecuting criminal offences. The bottom line is clear - those who are engaged in criminal activities cannot invoke the protection of personal data in order to prevent investigations related to their crimes!

A broader overview of GDPR is given in the literature (Rakovic, 2023). It should be noted that, in accordance with the GDPR, the key participants in the processing of personal data are the "Controller" and the "Processor" - the "Controller" determines the purpose and means of personal data processing, while the "Processor" processes personal data on behalf of the controller. As per GDPR, one of the key institutions is the "consent" of the data subject to the processing of personal data, as any form of freely expressed will of the data subject by which he or she, by statement or clearly affirmative action, approves the processing of personal data relating to him or her. A key problem that arises in the processing of personal data is "Personal Data Breach", which is a breach of security that leads to the accidental or illegal destruction, loss, alteration, unauthorized disclosure or access to personal data that is transmitted, stored or processed in another way.

The processing of personal data takes place in accordance with seven principles - legality, correctness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality and accountability (EU, 2016a; Rakovic, 2023). The essence is clear - personal data can be collected and processed only in accordance with the purpose for which they are intended and in the smallest possible scope, while they must be protected from all forms of abuse. In simple words, we need to "find the right measure" in the processing of personal data, and we know how difficult this is in many areas of life.

The GDPR defines eight key rights of data subjects (EU, 2016a) - the right to be informed about the processing of their personal data, the right to receive confirmation from the controller as to whether or not personal data have been processed, the right to correction, the right to deletion ("the right to be forgotten"), the right to ask the controller to limit processing, the right

to data portability, the right to object and the right not to be the subject of decisions based solely on automatic processing, including profiling.

The GDPR foresees very high penalties for violating the security of personal data, in two levels (EU, 2016a) - an administrative fine of up to €20 million, or up to 4% of the annual income in the previous financial year, i.e. €10 million, or up to 2% of the total annual turnover income in the previous financial year, which is more unfavorable for the perpetrator! The following are examples of fining operators for non-compliance with GDPR provisions in Europe, based on data available in the literature (Diligenski, 2019):

- Google fined €50 million in France for unclear purpose of processing personal data and forwarding personal data for marketing purposes without subject's consent.

- British Airways was fined €205 million in the UK, due to the loss of data for 500,000 customers due to a website compromise.

- Facebook was fined €100 million in Belgium because the "like" button was used to profile users in order to deliver advertisements to them.

- Facebook was fined €10 million in Italy for selling user data.

- Facebook was fined €565,000 in Great Britain for allowing Cambridge Analytics to use data from a survey of 300,000 users in Donald Trump's election campaign.

- Post in Austria was fined €10 million for profiling 3 million citizens in terms of political affiliations and selling data to political parties.

- Real estate company Deutche Wohnen in Germany was fined €14.5 million for keeping data on tenants for too long and without legal basis.

The above data refer to the year 2019, i.e. the first year after the full implementation of the GDPR. A similar trend continued after that period. For example, at the end of May 2022, the US Federal Commission fined Twitter €150 million because the company provided user information to advertisers, including phone numbers and e-mails, between May 2013 and September 2019, thereby misleading users to protect their personal data. Also, at the end of May 2023, after an investigation that has been conducted since 2020, company META (earlier Facebook) was fined €1,2 billion in Ireland due to the violation of European rules on data protection on the social network Facebook, because it transferred the personal data of users from the European Economic Area to the USA. The company was ordered to stop any transfer of personal data to the USA within 5 months.

It is interesting to analyze the relationship of the GDPR to the information security management standard ISO 27001. The analysis shows (Rakovic, 2023) that a correctly implemented information security management system according to the ISO 27001 standard **is still not sufficient** for compliance with the GDPR. Although there are many similarities between these documents, there are also significant differences. First of all, these documents differ in their character - the GDPR is a legally binding document, the non-implementation of which entails certain penalties, while the implementation of the standard is voluntary, until the organization opts for it. In addition, many institutions that exist in the GDPR do not exist within the ISO 27001 standard. This primarily refers to consent to the processing of personal data (Articles 7 and 8 GDPR), the right to erasure, i.e. "to be forgotten" (Art. 17 GDPR), the right to limit processing (Art. 18 GDPR), data portability (Art. 20 GDPR) and the right to object (Art. 21 GDPR), while the international transfer of personal data from Art. 46 of the GDPR partially exists in the ISO 27001 standard, but primarily refers to business data. On the

other hand, the standard contains details on maintaining the level of information protection, which is not present in the GDPR.

2.3. Law on personal data protection

In November 2018, the new Law on Personal Data Protection of the Republic of Serbia - LPDP (OGRS, 2018) was adopted. The constitutional basis for passing the Law in question is contained in Art. 42 of the Constitution (OGRS, 2006) which proclaims that the protection of personal data is guaranteed, that the collection, storage, processing and use of personal data are regulated by a separate law, that everyone has the right to be informed about the collected personal data and has the right to judicial protection in case of their abuse. In addition, this topic is dealt with in Art. 97 of the Constitution (OGRS, 2006) as part of the protection of freedoms and rights of citizens. The reasons for the adoption of the new LPDP lie both in internal needs to upgrade the legal system to better ensure the protection of personal data and in the context of joining the European Union, because the need to amend this Law was stated in 2016 as part of the report on Serbia's progress in the EU accession process.

The structure of the LPDP is shown in Table 3. This law essentially combined Regulation 679/2016 - GDPR (EU, 2016a) and Directive 680/2016 (EU, 2016b). A first glance at Table 3 indicates that in relation to the structure of the GDPR, sections VII "Cooperation and consistency" and X "Acts of delegation and implementation" are missing, which is a consequence of the fact that Serbia is not yet a member of the EU.

Table 3: The LPDP structure

Part	Title	Article	GDPR
I	Basic provisions	1-4	I
II	Principles	5-20	II
III	Rights of data subjects (data subjects)	21-40	III
IV	Controller and processor	41-62	IV
V	Transfers of personal data to third countries or international organizations	63-72	V
VI	Commissioner (Independent Supervisory Authorities)	73-81	VI
VII	Remedies, liability and penalties	82-87	VIII
VIII	Special cases of processing	88-94	IX
IX	Penal provisions	95	VIII
X	Transition and final provisions	96-102	XI

The principles of the LPDP and the GDPR and data subject rights in both documents overlap to a significant extent. There are certain differences between those documents (Rakovic, 2023):

- From the point of view of applicability, the GDPR has a significant advantage over the LPDP because it contains an extensive Preamble that accompanies the regulation itself and significantly contributes to its understanding through examples, explanations and the context of its adoption. The provisions from the Preamble were not included in the LPDP, and direct application of the GDPR is not possible because we are not a member of the EU, so in practice the provisions of the LPDP remain to be implemented in the spirit of other legislation.

- Both documents contain 26 definitions of which 22 overlap and 4 differ. The LPDP defined "person whose data are processed" (in the GDPR it is "data subject", but does not appear as a separate definition), "multinational company", "authorities" and "competent authorities", and omitted the definitions "mainly appointment of supervisory authority", "competent supervisory authority", "cross-border processing" and "relevant reasonable objection".

- The role of the supervisory body in the LPDP is taken over by the "Commissioner for Information of Public Importance and PDP".

- According to the LPDP, independent consent for the processing of personal data can be given by a person at the age of 15 (in the GDPR, 16 is recommended, but not younger than 13).

- The LPDP provides for the right to "complaint" to the Commissioner, the GDPR provides for the right to lodge an objection - appeal. Lawyers are united in their opinion that the legal effect of a complaint and an objection - appeal is not the same.

- Violations of the LPDP are subject to fines ranging from 50 thousand to 2 million RSD for 32 cases, as well as 6 cases with a fixed fine of 100 thousand RSD. It is drastically different from the GDPR because the range of fines is from €430 to €17,000. In a certain way it contradicts the view that the penal policy should act as a disincentive for offenders. The amount of the fines is far below the damage that can be caused by violating the LPDP and the profit that can be made in that way, so the violators calculate it as a "cost" of business!

It is interesting to consider the relationship between the LPDP and other regulations in the field of labor legislation in Serbia. The LPDP (OGRS, 2018) does not contain explicit provisions related to employers and employees, that is, the collection of personal data about the employee in the field of work, although in everyday work situations that require the processing of such data are frequent. Instead, Art. 91 of the LPDP (OGRS, 2018) refers to regulations in the field of work. In general, these issues are usually regulated by an employment contract or a collective agreement.

In practical application of labor legislation, it is necessary to take into account the following (Rakovic, 2023):

- That the data requested from job candidates be unambiguously related to the job position.

- That the data on the candidate who was not hired be stored for a future round of employment only if the candidate has unequivocally agreed to it.

- That medical data on the employee's state of health be limited to "remittances" confirming temporary incapacity for work, i.e. a doctor's opinion on temporary fitness for work, without details.

- That biometric data is collected only if it is necessary and if the purpose cannot be achieved in any other way (e.g. records of arrivals and departures from work).

- That data from the criminal record is collected only if it is prescribed in advance by law.

- That monitoring of employees is carried out when it is necessary (e.g. for their safety) and within the limits of "reasonably expected privacy", which is a concept developed by the European Court of Human Rights in its practice.

- That the monitoring of the employee's communication on the official phone or computer, that is, the official e-mail account, should be clearly declared in terms of the obligation to use these means of communication exclusively for business purposes, with a minimum of private communication.

- That the storage of employee data outside the Republic of Serbia, i.e. on "cloud computing" servers can only be carried out in terms of LPDP, because it has the character of presenting employee data.

2.4. Challenges and dilemmas in LPDP application

In the practical application of the LPDP, there are many dilemmas, inconsistencies and challenges, of which only the most significant are listed below (Rakovic, 2023):

- It was established a very short interval of 9 months from the entry into force of the LPDP until its implementation. In the case of the GDPR, that interval was 2 years. It was the reason why the Commissioner requested the postponement of the implementation of the LPDP from August 22, 2019. but this initiative was not accepted.

- The authorities often do not inform the Commissioner about relevant issues within his jurisdiction and often take steps without his consent. There are situations in which a large amount of data on Serbian citizens are transferred abroad, without approval of the Commissioner.

- There is still insufficient awareness among people about the importance of personal data. People usually think that they, as ordinary people, are not so important for someone to have some of their data, that they have nothing to hide, etc. In everyday life, it is possible to see that people themselves, in various forms (social networks, street surveys, public places and public transport, etc.) give their personal data to others without any need. Planned amendments to the LPDP and the adoption of the Personal Data Protection Strategy until 2030, are oriented to the introduction of education on personal data protection in primary and secondary schools.

- In the course of 2021 alone, more than 200 complaints about the violation of personal data were sent to the Commissioner (PDCS, 2021), and more than 300 inspections were carried out

- Banks or hotels often ask for an ID card, which, instead of basic identification, is read, printed and placed in some binders without any need, or kept at the reception desk during the guest's stay with the explanation that they are being asked to do so by the Ministry of Interior (MoI).

- By-laws did not resolve the issue of video surveillance in open and/or closed spaces (facial recognition technology), nor the issue of unauthorized use of photos on social networks.

- In the period from January 2015 to July 2020, the activities of the public prosecutor's office and the courts related to Art. 146 of the Criminal Code, which refers to the unauthorized collection of personal data (PDCS, 2021). The results show that out of 66 courts, in 14 there were a total of 28 cases related to that article, 4 acquittals, 2 convictions (both conditionally), and the other 22 cases were rejected as unfounded, dismissed or suspended. In the same period, the Commissioner submitted 17 criminal reports, but none of them received an epilogue, especially due to the fact that the injured parties often do not have lawyers due to their social and economic status.

- Within the unified information system (UIS) in education, there is a huge amount of data in the form of a register of students, their parents or guardians, a register of teachers, etc. as well as an electronic diary system. It was observed that the private firm that maintains that system on a commercial basis offers additional options to users in terms of access to the data of others. From the point of view of statistics, all the mentioned data should be anonymized, i.e. that data on real persons can only be seen in special databases, which are not widely available.

- In the LPDP, art. 12, six bases are defined on which personal data can be processed while respecting the principle of legality of processing. The most flexible basis in practice is the

basis of processing which is based on the legitimate interests of the operator or a third party, unless the interest of the person whose data is being processed prevails over them. The dilemma remains, where is the line where the legitimate interest ends and the private interest of the person whose data is processed begins. In general, this basis of processing requires a more careful and analytical approach, all in the context of the "reasonable expectations of the individual", as defined in paragraph (47) of the GDPR Preamble (EU, 2016a).

- At the time of the COVID-19 pandemic, healthcare came into focus because in some areas, data on the health status of people became publicly available on the websites of local governments. In this area, it was not clear who is the handler and who is the processor, and what is the legal basis for collecting, processing and disclosing that data. A drastic example is the situation when RTV Pink published a video lasting several minutes from the KCS Infectious Diseases Clinic showing several patients on ventilators whose faces were visible.

- A special segment related to the collection and processing of personal data is represented by companies - organizations that carry out these activities on the basis of the legal obligation to record the employment relationship, for the purpose of realizing the rights of employees and their family members or for the purpose of realizing the business and legitimate interest of the organization (e.g. employee references as part of the bidding and contracting process). In this sense, the principles of minimization (collecting only as much data as is necessary, no more and no less) and expediency, i.e. that for each of the data there is a clear purpose for which it is collected and processed (Reljanovic, 2020).

- In practice, there are many cases of abuse of personal data in order to discriminate against sensitive groups, e.g. women for whom, during employment, the employer requests information that is not of interest to the job, such as information on marital status and family planning, or information related to health, an extract from criminal records, etc.

3. CASE STUDY: ENTEL

The application of personal data protection is illustrated on the example of the company Energoprojekt Entel plc, Belgrade. It is the company whose activity is design, consulting and engineering in the fields of energy, water, telecommunications and environmental protection. The organization has implemented an integrated management system (IMS) with five management standards - quality, environmental protection, safety and health at work, information security and energy management, in accordance with the relevant ISO standards (EPE, 2022).

Starting from the previously stated position that a correctly implemented information security management system according to ISO 27001 is not sufficient for the full implementation of the provisions of the GDPR, i.e. the LPDP, the organization expanded its information security management system (defined by procedure EN-27P-01) with a special procedure EN-27P-02 which is dedicated to the topic of personal data protection. The subject procedure regulates:

- Analysis (mapping) of personal data (data description, category, basis of processing, storage period, medium/location of storage, transfer to a third party, controller, processor and a more detailed description of the purpose of processing).

- Assessment of the impact on the security of personal data.

- Procedure in case of endangering the security of personal data.

- Giving and revoking consent to the processing of personal data.

- Gaining insight into the employee's personal data that is collected and processed about him.

- Erase personal data.

The procedure has totally seven forms (EPE, 2022) - personal data register, personal data security impact assessment, personal data security impact assessment procedure, statement of consent to personal data processing, statement of revocation of consent to personal data processing, a request for insight into the personal data being processed and an order - a list for erase personal data.

In addition to employees, this procedure includes the collection and processing of personal data of potential employees (who apply for a job through the organization's website) and suppliers and other business partners.

For the sake of illustration, below are listed several key decisions that the company made as part of defining the system for the protection of personal data:

- From the register of personal data, all items that could be disputed from the point of view of protection of personal data, such as the reading of an identity card, a copy of a passport as a biometric data, etc., have been omitted. For each of the items, the purpose of collection and processing is stated.

- It is defined that the official phone, computer, or official e-mail account can be used exclusively for official purposes and that the distribution of inappropriate content through these means is subject to disciplinary responsibility.

- That the data about the candidate who applied through the company's website, but was not hired, is stored for a future round of employment within a period of 12 months from the moment of application, and that it is removed after that time. The potential employee is informed about this fact in the process of applying to the site.

- Although the procedure envisages giving consent to the processing of personal data, in practice it is decided not to collect anything that would be subject to the obligation to give consent for processing. In the procedure, it is explicitly stated that the registration of children for New Year's packages, i.e. for traditional prizes for students for success achieved at school, is considered as giving consent that their names can be found on the list of persons to whom those gifts were given.

- Data on Unified Identification Number of Citizens (UINC) for employees exist within the information system, but access to that data is enabled to a small number of employees, primarily the specialists of professional services and the top management of the company.

4. CONCLUSION

In this paper, the topic related to the protection of personal data is considered from the point of view of the information security management standard ISO/IEC 27001, European regulations and laws in the Republic of Serbia. Also, some challenges, dilemmas and experiences in application of standards and regulations are discussed. It is necessary to mention that the topic is still new in our conditions and is particularly burdened by the tendency of our mentality to avoid, rather than implement, established rules. It is crucial to take measures of a preventive nature, and not to treat the consequences when problems arise. In practical application, there are many difficulties, considering that many elements are not defined by secondary legislation (use of UINC, video surveillance outdoors - traffic, parks, and indoors - shopping centers, etc.). It is very important to strengthen people's awareness of the protection of personal data, as well as their constant education in this area. The fact is that there is a lot of possibilities for improvement, but it requires time, effort and patience.

REFERENCES

Diligenski. A. (2019). Bulletin of lawyers - practitioners, no. 9, December 2019: "Institutions in Serbia are not prepared for the new Personal Data Protection Act", www.kolega.rs, [Accessed 30/05/2023]

EPE. (2022). Energoprojekt Entel plc IMS documents

EU (2000). Charter of Fundamental Rights of the European Union, Official Journal of European Union C 364/01, 18.12.2000

EU (2016a). Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJEU, 4.05.2016, L 119/1 to 88)

EU (2016b). Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (OJEU, 4.05.2016, L 119/89 to 130)

ISO (2022a). Information security, cyber security and privacy protection - Information security management systems - Requirements (ISO 27001)

ISO (2022b). Information security, cyber security and privacy protection - Information security controls (ISO 27002)

OGRS (2006). Constitution of the Republic of Serbia (Official Gazette of Republic of Serbia 98/2006, 115/2021 and 16/2022)

OGRS (2018). Law on Personal data protection (Official Gazette of Republic of Serbia 87/2018, 13.11.2018)

PDCS (2021), Privacy and protection of personal data in Serbia – Analysis of selected sectoral regulations and their application (Partners for Democratic Changes Serbia, #EU for you, Ministry for Human and Minority Rights and Social Dialogue, Belgrade, March 2021)

Rakovic, R. (2023). Personal data protection – Framework and challenges, Belgrade: Engineering Academy of Serbia (in Serbian)

Reljanovic, M (2020). „Protection of personal data in the employment relationship“ (Personal data protection in Serbia - Proceedings, Institute for Comparative Law, Belgrade, 2020, pp. 61-92 (in Serbian)

UN (1948). Universal Declaration of Human Rights, UN