Rewiew

THE RIGHT TO PRIVACY AND THE PROTECTION OF PATIENTS' PERSONAL DATA

Katarina Jonev Ćiraković

Medika College of Vocational Studies in Healthcare, Belgrade, Serbia

Received: December 20**,** 2023**; Revised**: November 10, 2024.
Accepted: November 12, 2023; **Published:** November 17, 2024.

DOI: 10.5937/annnur2-48334

Abstract

Globalization and accelerated technological development have led to new challenges in the protection of personal data. The Internet holds vast amounts of information, which at any moment is at risk of potential misuse on various websites, social networks, and platforms. The adoption of the EU General Data Protection Regulation (GDPR) marked a significant step in addressing this issue. Data related to the health sector—specifically, patients' personal data—are particularly sensitive. The concept of personal rights and their protection stems from the belief in universal values that apply to every individual. Safeguarding patient privacy is essential for preserving freedom and upholding fundamental human rights. It is crucial to define the scope and limitations of this protection, balancing the legitimate interests of third parties, society, and the state on one side, with the individual rights and interests of the patient on the other. In this context, recent amendments in European and Serbian legislation regarding personal data protection represent a cornerstone for this research, which holds significance for both legal and medical science, as well as practical application.

Keywords: patient rights, healthcare, internet, data protection

Corresponding Author: Katarina Jonev Ćiraković; E-mail: jonev.katarina@gmail.com

Introduction

One of the most significant consequences of advancements in information technology over the past twenty years is the massive increase in data collected on individuals. The daily collection of billions of data points about citizens, their storage in large databases, and the processing of this data using artificial intelligence have become everyday realities. As the volume of data collected on individuals grows, so does the risk of its misuse.

The free flow of information is essential, but it also poses a significant risk to the privacy, independence, and individuality of everyone. Placing data at the core of industrial development and societal management demands a high level of both information security and protection of citizens' fundamental rights. A robust personal data protection system must address both the technical aspects of securing information systems and the coordinated regulatory framework and practical application of personal data protection at the international and national levels.

A significant step forward in the creation of a personal data protection system was the adoption of the EU General Data Protection Regulation (GDPR). This regulation not only harmonized norms and practices at the EU level but, since its implementation in 2018, has greatly influenced the development of data protection systems in candidate countries.[1] The GDPR has had a global impact on the evolution of data protection systems, including in the Republic of Serbia. Under the influence of the GDPR, Serbia adopted a new Law on the Protection of Personal Data.[2] The GDPR warrants special attention across various fields—legal, economic, accounting, healthcare, auditing, and all other areas of the digital business environment.

The protection of personal data, as required by numerous international and national regulations, is crucial for safeguarding an individual's right to privacy. The right to personal data protection and the right to respect for private life are closely related fundamental rights. Patient health data is a vital aspect of privacy, categorized as highly sensitive information. Therefore, processing such data requires special care and must always be conducted with respect for the interests, fundamental rights, and dignity of the person to whom the data belongs. By protecting an individual's health-related data, we safeguard their legitimate interests. This protection involves preventing the misuse of personal health information, such as illegal or unjustified access and use.

The development of information and communication technologies (ICT) and their increasing application in healthcare sector has made it possible to collect and process a large amount of health data of persons, which opened the issue of their security and protection. ICT in the healthcare sector offers numerous new opportunities in terms of better and more responsible healthcare for individuals (consumers, patients, doctors and healthcare workers), but it also has disadvantages that can negatively affect the rights of individuals, their privacy and the protection of personal data. This may pose a particular risk to the protection of the right to privacy and data protection due to misuse - illegal and unjustified use and/or disclosure of that data.

What is Included in the Patient's' Medical Records?

Health-related data are considered a professional secret for all entities involved in the process of ensuring a patient's right to health care. Unauthorized disclosure of this data can lead to disciplinary, administrative, civil, misdemeanor, and even criminal liability. Furthermore, because patient medical data may be accessible to multiple parties, it cannot be disclosed to the public without the consent of the patient or individuals authorized by law.[5]

To understand the protection of a patient's right to privacy and the potential liability of the health care institution, it is important to first examine what constitutes medical data that guarantees the right to privacy.[6]

According to one definition accepted in both European and Serbian law, health data is personal data related to an individual's physical or mental health, including information about the provision of health services, from which details about their health condition can be derived.[2]

In addition to the aforementioned data, any other information obtained during the diagnostic and treatment process, or in connection with the applied treatment procedures, is considered personal and must not be disclosed to third parties. The unauthorized transfer of such data would constitute a violation of the right to privacy and could compromise the patient's integrity. While the scope of this data is defined, it is not exhaustive, as new types and even categories of data related to the patient's health condition and treatment may emerge. In this context, a special category of data related to the patient's genetic status is particularly noteworthy.[6]

Advances in biotechnology have made it possible to analyze human genetic material to protect, preserve, and enhance health. As a result, additional measures are necessary to prevent abuses related to the possession, use, and disposal of a patient's genetic information, which is classified as a special category of health-related data.

At the European and national level, there is a whole range of instruments that regulate in detail various aspects of the right to privacy and confidentiality. Nowadays, in personalized medicine era, in the era of the digital economy and with the development of information and communication technologies, new challenges are emerging on how to protect data on the health status of employees as patients who are very vulnerable and suitable for endangerment.[7]

The Right to Privacy of Patients

In the modern digital world, where e-health is increasingly advancing, personal health data holds significant value. Without such data, e-health could not have been created, nor could it continue to develop and adapt to the constant changes in modern society and the digital environment. Health services provided to patients must be legally regulated and free from any arbitrary influence by those who administer them.

The right to privacy of patients stems from the general right to privacy, which includes the right to protect personal data and serves as "an additional guarantee of the inviolability of human integrity." In the broadest sense, the right to privacy allows individuals to decide what information about themselves may be disclosed to

others, how this information will be collected, and for what purpose it will be used.[9] The right to privacy is a fundamental human right essential to the functioning of both the state and society. This right is partof the corpus of personal rights, which emerged in the United States legal doctrine at the end of the 19th century. It protects the private sphere of an individual—encompassing physical, mental, and informational aspects (the collection, processing, use, and protection of personal data are regulated by law).[10]

The state's role in guaranteeing this right is twofold: both passive and active. The state must refrain from intruding into an individual's private sphere, while simultaneously establishing laws to ensure the right to privacy. Given that privacy is a personal right of citizens, theoretical frameworks often distinguish between different spheres of privacy—namely, the intimate sphere, the strictly personal sphere, and the private-public sphere, which lies between the first two categories. [11]In the context of citizens' medical and health data, we are specifically referring to the strictly personal sphere of privacy.[12]

The right to privacy in healthcare is realized through the legal protection of a patient's personal (confidential) health data, irrespective of the type of health insurance—whether compulsory, voluntary, or otherwise. Privacy involves the duty to maintain the confidentiality of personal health data, where the right to confidentiality allows individuals to prevent the unauthorized re-disclosure of sensitive personal information to third parties. Confidentiality forms the foundation of the doctor-patient partnership, which, in modern law, replaces the earlier paternalistic approach and serves as a prerequisite for delivering quality medical services.[13]

While ensuring the confidentiality of a patient's health information is a duty of the doctor, it also represents the patient's right to have their personal data legally protected. The patient's rights to privacy and confidentiality of health information are closely tied to the right to personal data protection, a constitutionally guaranteed right; these rights are mutually dependent and interrelated. It is especially important that the patient's personal data is legally protected during processing. This responsibility also extends to healthcare professionals, who are obligated to safeguard the life, health, privacy, and dignity of each patient.

Many healthcare workers and associates participate in the treatment process and must be informed about the patient's health status to effectively perform their duties and carry out necessary procedures. Specifically, the details about a patient's health status, acquired during professional responsibilities, are subject to legal protection.

Data Protection in Information Health System

Over the past three decades, the level of regulation in data protection and cybersecurity has significantly increased. To ensure effective governance, it is essential to differentiate between sector-specific laws that regulate health data processing, general data protection laws (such as GDPR), and laws that govern personal data processing, which may have direct or indirect implications for health information systems (e.g., e-Privacy).

Sector-specific regulation laws are crucial as they provide clear guidelines for processing personal data for health-related purposes and often serve as the legal foundation for such activities. These laws may address specific public health tasks

(e.g., cancer registries) or regulate the use of health information in clinical or medical settings (e.g., electronic health records), with subsequent secondary use of the data for public health purposes. Data protection necessitates the development and implementation of such laws, as they help ensure maximum transparency and democratic legitimacy.[14] The application of general data protection laws, particularly broader legislation, presents significantly greater challenges in the context of health information systems.

Under general data protection legislation, the processing of personal data for health purposes is privileged. This applies not only to the processing of data for health protection ("vital interest") but also to the use of personal data for public health purposes. For example, the introductory statement of Article 46 of the GDPR states: "The processing of personal data shall also be considered lawful when it is necessary to protect an interest that is essential to the life of the data subject or another person".[15]

Certain types of processing may also serve important public interest grounds and vital interests of the data subject. This includes, for example, processing necessary for humanitarian purposes, such as monitoring epidemics and their spread, or in situations of humanitarian emergencies, particularly during natural disasters or man-made catastrophes.

While information security has traditionally focused on data integrity and availability, data protection has been primarily concerned with processing confidentiality. In recent years, these areas have increasingly converged, with regulatory acts such as the GDPR imposing strict data security requirements on data controllers.[16]

The regulation specifies that personal data refers to any information relating to an individual whose identity is either already determined or can be determined.[17] An identifiable individual is one who can be directly or indirectly identified through an identifier, such as a name, identification number, location data, network identifier, or through one or more factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.[18]

It can be concluded that the EU General Data Protection Regulation applies exclusively to living natural persons (not legal entities) whose identity can be determined based on certain personal characteristics. This means the Regulation does not apply to individuals who cannot be identified or who present themselves under a false identity, which is particularly relevant in the context of the internet community and individuals who "hide" behind fake online profiles.[19]

Since its primary focus is protection, the Regulation specifies what constitutes a violation of privacy. A privacy violation refers to any security breach that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to data that has been transmitted, stored, or otherwise processed.[18] Therefore, legal compliance requires that any activities involving the processing of personal data must adhere to the provisions of the EU General Data Protection Regulation and respect basic human rights and freedoms.

Data processing refers to any activity or set of activities performed on personal data or sets of data, whether automatically or manually. This includes actions such as collection, recording, organization, structuring, storage, modification, retrieval, inspection, comparison, disclosure by

transfer, dissemination, or otherwise making data available, as well as matching, combining, restricting, erasing, or destroying data.[19] In essence, this means that any use or handling of data can be classified as a processing operation. This means that controllers (and processors) must implement appropriate security measures to prevent the accidental or intentional compromise of the personal data they hold. Controllers should recognize that while information security is often equated with cybersecurity (protecting networks and information systems from attacks), it also encompasses other aspects, such as physical and organizational security measures. Effective organizational and technical measures to protect personal data are crucial for maintaining the trust of individuals whose data is processed, and they will help public health systems secure public support and cooperation from data subjects.

Measures may include not only technical solutions—such as encrypting data both at rest and in transit—but also a comprehensive approach to identity and access management or data governance, which involves classifying data (e.g., as Top Secret, Confidential, or Public). A key aspect of protection is the strict management of administration and access rights. Public health institutions—and healthcare institutions in general—often fail to enforce a stringent "need to know" principle.

Regulations like the GDPR do not specify exact security measures. Instead, they require controllers to implement a level of security that is "appropriate" to the risks posed by the processing. Public health authorities and other stakeholders in the sector should take this into account, considering the latest developments, implementation costs, and the nature, scope, context, and purpose of the process.

Given that the public health sector is often tasked with processing sensitive personal data, such as health and physical well-being information, data subjects will expect a very high level of security for such operations. Additionally, a lack of funds for data security measures is not an excuse, provided those measures are necessary to achieve an "adequate" level of protection.

An important issue is how to handle data compromises that lead to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data. This includes injuries resulting from both accidental and intentional acts. Institutions of any size or setting can easily become overwhelmed by a data breach. Therefore, public health institutions are advised to plan for such eventualities, potentially conducting cyber incident simulations. A data breach plan is essential, with a clear allocation of tasks and responsibilities, including a communication strategy for breaches.

An important tool in this effort is regular penetration testing, conducted by an independent third party.[20] In simple terms, the data controller should invite "ethical hackers" to identify weaknesses in the system. Many countries have IT security or cybersecurity agencies that can assist public health institutions in establishing these protocols. For institutions that serve operational purposes, a disaster recovery plan is also critical and demanding.

Protection of Patient Data

Personal health information is a critical element of privacy. This data represents a special and very sensitive category of information. Therefore, the processing of such data is particularly sensitive and must always be conducted in a way that preserves the interests, fundamental rights, and dignity of the individual whose data is being processed. The right to the protection of personal health-related data is the right to protect an individual's legitimate, moral, and economic interests. This includes safeguarding personal health data from the risk of misuse, as well as from unconstitutional, illegal, or unjustified access and use, and from sanctioning illegal use and abuse.[21] Individuals (patients) are increasingly losing control over personal data related to their health condition.

Numerous EU regulations include provisions on the protection of an individual's data related to their state of health. However, there is currently no regulation that specifically addresses the issues of personal data protection related to health at the European level. The GDPR aims to facilitate the flow of health data while ensuring the protection of personal (health) data from the risk of misuse, as well as from all illegal, unwanted, and unnecessary access and use of that data. In other words, a high level of protection for health-related personal data must be ensured. It is essential to continually strengthen and develop new technologies and monitoring mechanisms that enable the detection and sanctioning of potential violations of the fundamental right to the protection of personal data related to health.[22]

Health services provided to patients for different purposes must be legally regulated. The obligation of confidentiality and storage of personal data about the patient and his health condition opens several important, complex and sensitive legal and ethical issues. The successful development of cross-border health services also depends on the trust of the users of these services (patients) that their privacy will not be compromised, that is, that their health data will be used and protected in an appropriate manner.[23]

Directive 2011/24/EU on the application of patients' rights in cross-border healthcare (hereinafter referred to as Directive 2011/24/EU) addresses the cross-border transfer and protection of personal data related to patients' health. This Directive establishes rules to facilitate access to safe and high-quality cross-border healthcare and to promote cooperation in the healthcare sector between member states, while fully respecting national competencies in the organization and provision of healthcare.[24] According to Article 14 of Directive 2011/24/EU, the Union supports and facilitates cooperation and the exchange of information between member states, acting as part of a voluntary network that connects state authorities responsible for e-health, as appointed by the member states.

The goals of the e-health network are to: (1) provide sustainable economic and social benefits of European e-health systems and services, with interoperable applications aimed at achieving a high level of trust and security, improving the continuity of healthcare, and ensuring access to safe and high-quality healthcare; (2) develop guidelines on a standardized list of data to be included in patient summaries for use by healthcare professionals to enable continuity of cross-border healthcare and

ensure patient safety; (3) establish effective methods for enabling the use of medical data for public health and research purposes; and (4) support member states in developing common measures for identification and verification to facilitate the secure transfer of data in cross-border healthcare.[23] These goals are pursued with full respect for data protection principles as stated in Directives 95/46/EC and 2002/58/EC.

The protection of personal data, as mandated by numerous international and national regulations, is crucial for safeguarding the right to respect private life. The right to personal data protection and the right to respect for private life are two distinct yet closely related fundamental rights.

According to the established practice of the EU Court, the right to personal data protection must be balanced with other fundamental rights. This right is essential for ensuring respect for private life.

Personal health information is a critical aspect of privacy. This information constitutes a special and highly sensitive category of data. Therefore, the processing of such data is particularly sensitive and must always prioritize the interests, fundamental rights, and dignity of the individual whose data is being processed. The right to protect personal health-related data includes the protection of an individual's legitimate, moral, and economic interests. This encompasses safeguarding personal health information from risks of misuse, as well as from unconstitutional, illegal, or unjustified access and use, with appropriate sanctions for illegal use and abuse.[21] However, individuals (patients) are experiencing decreasing control over personal data related to their health condition.

Numerous EU regulations include provisions for protecting an individual's health-related data. However, there is currently no regulation specifically addressing personal data protection in healthcare at the European level. Implementing the GDPR is essential not only for the effective operation of healthcare services but also for safeguarding the rights of both employees and patients. In the healthcare sector, personal data is continuously collected, processed, and stored, encompassing everything from patient health records to sensitive employee information. Without robust data protection measures, there is a substantial risk of unauthorized access, data breaches, or misuse, which can erode trust in healthcare systems and jeopardize individuals' privacy.

For patients, the GDPR safeguards their personal and health-related data, giving them control over who accesses their information and how it is used. It provides them with the right to know what data is being collected, the ability to request corrections, and the right to withdraw consent. For healthcare employees, the GDPR ensures that their personal data is handled responsibly, granting them rights like those of patients in terms of privacy protection. Additionally, implementing the GDPR in healthcare is essential for maintaining compliance with European standards, promoting transparency, and building trust between healthcare providers and patients. It encourages healthcare institutions to adopt best practices in data protection, which not only upholds individuals' rights but also strengthens the integrity and efficiency of healthcare services.

The GDPR should facilitate the flow of health data while simultaneously protecting personal (health) data from misuse, as well as from any illegal, unwanted, or unnecessary access and use. In other words,

a high level of protection for health-related personal data must be ensured. It is essential to continually strengthen and develop new technologies and mechanisms for detection and monitoring, which in practice enable the identification and sanctioning of potential violations of the fundamental right to personal data protection in relation to health.

Article 17 of the Personal Data Protection Act classifies data from health records as highly sensitive. The same article stipulates that processing data that reveals the health status of an individual is prohibited. Exceptions to this prohibition are allowed if the processing is necessary for purposes such as preventive medicine, medical diagnostics, assessing the working capacity of employees, providing healthcare services, improving the healthcare system, or fulfilling public interest in the field of public health. In these cases, data processing is permitted, but only with the application of appropriate measures to protect the rights of the individuals concerned. This means that issues arise when personal data protection measures are not implemented, allowing everyone access to the most sensitive data, even with patient approval.

Healthcare workers play a critical role in safeguarding personal health data. Accordingly, they have a strict duty to maintain the confidentiality of any data they acquire in the course of their work. However, they may be exempt from this duty only with the written consent of the patient or their legal representative, or by decision of the competent court.

Protection of Patient Data in Serbia

The digitization and advancement of technology, the growing use of data across various fields, and new regulatory acts introduced in Europe have prompted Serbia to take legislative action on personal data protection. As a result, in 2018, Serbia adopted the Law on Protection of Personal Data, replacing the previous law that had been in effect since 2008.[2]

With the increasing number of digital platforms and data processing systems involving health information, there is a real risk of data misuse, which could have serious consequences for patients' privacy and security. Therefore, it is essential to enhance the protection of this data and establish legal mechanisms to ensure its security.

The Law on Patients' Rights of the Republic of Serbia[25] includes provisions that define patients' rights to access healthcare and the means by which these rights can be exercised and protected. These provisions are directly related to the protection of patient privacy and represent a form of realizing the right to patient privacy. The law specifically addresses patients' rights to privacy and confidentiality, guaranteeing the right to privacy regarding all personal information shared with healthcare professionals or associates. This includes information about their health condition, potential diagnostic and therapeutic procedures, as well as the right to privacy during diagnostic tests and treatment (Article 14). Patients are guaranteed the right to privacy and confidentiality of all personal information communicated to the responsible healthcare professional or associate, including details about their health condition and any diagnostic or therapeutic procedures, as well as the right to protect their privacy throughout the diagnostic and treatment process.

Patients have the right to access their medical records, and denial of this access constitutes a violation of their right to privacy and confidentiality. However, this access must not disrupt established procedures within healthcare and other

institutions that must be followed when exercising the right to review records (Article 20). In cases where the patient is a child or a person deprived of legal capacity, the legal representative has the right to access the medical records. A child who has reached the age of 15 and possesses mental capacity also has the right to access their own medical records.

The healthcare professional in charge is responsible for properly maintaining medical records in compliance with the law. They must document all medical measures taken for a patient, including: the case history, diagnosis, diagnostic procedures, therapy, therapy outcomes, and any advice given to the patient (Article 20).

The right to confidentiality of patient health data: Health status data, or data from medical records, is considered personal and particularly sensitive information under the law. Individuals who unlawfully handle or disclose this data without the patient's or legal representative's consent, thereby violating this Article, are held accountable for the unauthorized disclosure of sensitive data in accordance with the Law (Article 21).

Health professionals, health associates, and other employees working under the employer's authority may only be relieved of their duty to safeguard this data in accordance with the Law, and only upon written consent from the patient or their legal representative, or by a court decision. If the patient or legal representative provides a written statement or authorization, notarized by the competent authority and kept in the medical records, granting consent for the disclosure of health information, the responsible health professional may disclose details about the patient's health condition. Additionally, the competent health professional may disclose information about the patient's health to an adult member of the immediate family if the patient has not given consent, provided this disclosure is necessary to avoid potential health risks to the family member (Article 22).

The patient or their legal representative is entitled to a copy of medical records, with the costs of duplication covered by the patient or representative. Copies of records for a deceased family member may be provided to an adult family member or legal representative upon request for legal purposes. Medical data or copies may be shared with certain entities, such as health insurance organizations and judicial authorities, when required by law. Additionally, medical records may be used for scientific research with the patient's consent, with all data handled as particularly sensitive personal information in compliance with legal standards (Article 23).

In the case of the Republic of Serbia, it is important to mention an obligation of the Institute for Public Health regarding data breaches. This obligation is a special rule in relation to the general data protection system. Specifically, the Institute for Public Health is required to notify the person to whom the data pertains, the ministry responsible for health affairs, and the Commissioner of any violation of the security of personal data.

The purpose of notifying healthcare institutions and individuals is to act efficiently and from different perspectives on the injury, preventing its negative effects. This is particularly important because the data involved can reveal sensitive personal information that could affect an individual's personal, professional, and social position or status. If the Institute of Public Health fails to inform these parties about the violation, it may face a fine ranging from 50,000 to 2,000,000 dinars.

Patients have the right to access their personal data stored in medical records. The option to review this data should also be available online, but only if the data protection measures outlined in the Law on the Protection of Personal Data are ensured. Security and safety measures must be implemented by all healthcare institutions, private practices, and other legal entities within the medical sector.

Conclusion

One of the significant consequences of the development of information technologies over the past twenty years is the enormous increase in the amount of data about individuals. The free flow of information is both a necessity and a great danger to privacy, independence, and individuality.

A significant step forward in creating a personal data protection system was the adoption of GDPR. This regulation not only harmonized norms and practices at the EU level but, since its implementation in 2018, has had a major impact on the development of data protection systems in many countries around the world, including Serbia.

Patient health data is a critical element of privacy. This data is a special, highly sensitive category of information. Therefore, the processing of such data is particularly sensitive and must always be carried out in a way that preserves the interests, fundamental rights, and dignity of the individual whose data is being processed.

Establishing a strong, clear, and modern framework for data protection in the EU and Serbia that can address the numerous challenges of the modern digital age and the global digital market, while raising the culture of privacy and protection of personal data to a higher level, is essential.

Conflict of Interest

The author declares no conflict of interest.

References

1. Daigle B, Khan M. The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities. United States International Trade Commission Journal of International Commerce and Economics. 1-38. 2020: https://www.usitc.gov/publications/332/journals/jice_gdpr_enforcement.pdf / Last access on November 1, 2023.

2. Law on the of Personal Data, Official Gazette of the Republic of Serbia, No. 87/2018.

3. Grozdanić V, Škorić M, Ritosa D. Liječnička tajna u funkciji zaštite privatnosti osoba s duševnim smetnjama, Zbornik Pravnog fakulteta u Zagrebu, vol. 64., br. 5-6., 2014., pp 835. Available at: https://core.ac.uk/download/pdf/197800485.pdf /Last access on November 7, .2024.

4. Stojković-Zlatanović S, Lazarević B. Poverljivost podataka o ličnosti-implikacije na položaj zaposlenih sa stanovišta sudske prakse", Pravo i privreda, br. 4-6/2017, pp 706. Available at: https://scindeks.ceon.rs/article.aspx?artid=0354-35011706702S /Last access on November 5,2024.

5. Brković R, Jovanović Z, Totić M. Pravo na privatnost i zaštitu ličnih podataka zaposlenog kao pacijenta u pravu Republike Srbije", 2020, pp 205. Available at: https://www.researchgate.net/publication/339784081. Last access on November 8, 2024.

6. Stojković Zlatanović S, Sovilj R. Pravo na privatnost i zaštita genetskih informacija u oblasti rada i zapošljavanja. Srpska politička misao 2017; 58 (4): 1-20 Available at: https://www.academia.edu/42169645/ Last access on November 11, 2024.

7. Mujović Zornić H, Petrović Z. Odgovornost zdravstvenih ustanova za štete kao posledice lečenja, Vojno-sanitetski pregled, 2012; 69 (8): 692-699. Available at: http://www.vma.mod.gov.rs/vsp_08_2012.pdf / Last access on November 8,2024.

8. Marković R. Ustavno parvo. Pravni fakultet, Beograd: Univerzitet u Beogradu, 2018; pp 475.

9. Westin A. Social and Political Dimensions of Privacy. Journal of Social Issues 2003; 59 (2): 431-453. DOI: https://doi.org/10.1111/1540-4560.00072

10. Radišić J. Medicinsko parvo. Beograd: Nomos; 2008, pp 223.

11. Warren SD, Brandeis LD. The Right to Privacy. Harvard Law Review 1890; 4 (5): 193 – 220. Available at: https://docenti.unimc.it/benedetta.barbisan/teaching/2017/17581/files/the-right-to-privacy-warren-brandeis / Last access on November 7,2024.

12. Klajn Tatić V. Profesionana tajna zdravstvenih radnika i razlozi za njeno otkrivanje. Strani pravni život, Institut za uporedno pravo, Beograd br. 3/2014, 225 – 244. Available at: https://www.stranipravnizivot.rs/index.php/SPZ/article/view/226 /Last access on November 6, 2024.

13. Constitution of the Republic of Serbia, Official Gazette of the Republic of Serbia, No. 98/2006 and 115/2021

14. Voigt P, von dem Bussche A. Rights of data subjects. In: The EU General Data Protection Regulation (GDPR). Cham: Springer; 2017: pp 141–87. DOI: https://doi.org/10.1007/978-3-319-57959-7

15. Chapter 6.1 of Handbook on European data protection law – 2018 edition. Vienna: European Union Agency for Fundamental Rights; 2018 Available at: https://fra.europa.eu/en/publication/2018/ handbook-european-data-protection-law-2018-edition).

16. Handbook on security of personal data processing. Athens: European Union Agency for Cybersecurity; 2018 Available at: https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

17. Voigt Paul, Dem Bussche Axel, The EU General Data Protection Regulation (GDPR)- A Practical Guide, Springer eBook, online 2017. Available at: https://www.scribd.com/document/369822372/The-EU-GDPR-A-practical-Guide-Paul-Voigt-pdf

18. Genaral Data Protection Regulation Available at: GDPR https://eur-lex.europa.eu/eli/reg/2016/679/oj.

19. Andonović S, Prlja D ,,Osnovi prava zaštite podataka o ličnosti", Beograd: Institut za uporedno parvo; 2020, pp 97.

20. Wilmslow: Information Commissioner's Office; 2020. Available at: https:// ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ personal-data-breaches/?q=data+breach. Last access on December 1,2023.

21. Peeters M. Free Movement of Patients: Directive 2011/24 on the Application of Patients' Rights in Cross-Border Health care. European Journal of Health Law 2012; 19 (1): 29-60, DOI:https://doi.org/10.1163/157180912x 615158

22. Bevanda M, Čolaković M. Pravni okvir za zaštitu osobnih podataka (u vezi sa zdravljem) u pravu Evropske Unije, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, 2016; 37(1), 125-154. DOI: https://doi.org/10.30925/ zpfsr.37.1.5,

23. Orentlicher D. Prescription Data Mining and the Protection of Patients' Interests. Journal of Law, Medicine & Ethics 2010; 38 (1): 74-84. DOI: https://doi.org/10.1111/j.1748-720X.2010.00468.x

24. General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

25. Law on Patients' Rights, "Official Gazette of RS", no. 45/2013 and 25/2019 .