

Patient's Right to Protection of Personal Data in the Legal System of Bosnia and Herzegovina

MARKO BEVANDA & MAJA ČOLAKOVIĆ

Abstract Health-related personal data belong to a category of sensitive data which, therefore, must be specially protected. The protection of personal health data is one of the patients' fundamental rights. Doctors protect their patients' interests only when the information gained about patients, while providing them medical treatment, are kept secret. In this paper, the authors provide an overview of the legal framework for the protection of health-related personal data in the legal system of Bosnia and Herzegovina. In addition to the analysis of the relevant legal provisions and considering the situation in practice, it can be concluded that formal harmonisation of legislation with the *acquis communautaire* in this field is not followed by effective implementation of regulation in practice.

Keywords: • privacy • doctor • medical malpractice • liability for damage •

CORRESPONDENCE ADDRESS: Marko Bevanda, Ph.D., Associate Professor, »Džemal Bijedić« University of Mostar, Faculty of Law, Matice Hrvatske bb, 88 000 Mostar, Bosnia in Herzegovina, email: marko.bevanda@pfmo.ba. Maja Čolaković, Ph.D., Associate Professor, »Džemal Bijedić« University of Mostar, Faculty of Law, Univerzitetski kampus bb, 88 104 Mostar, Mostar, Bosnia in Herzegovina, email: maja.colakovic@unmo.ba.

DOI 10.18690/24637955.10.1.1-17(2017) ISSN 2463-7955

© 2017 University of Maribor Press

Available at <http://journals.um.si/>

1 Introduction

1.1 Doctor-patient relations in terms of the patient's privacy protection

Health service is comprised of a number of components: legal, ethical, economic, social etc. The legal relationship between a provider and a recipient of health services is extremely complex,¹ but its ethical dimension is of essential importance (Donev, 2013: 503-512).

The relationship between a doctor, as a fundamental, independent and responsible provider of healthcare, and a patient is particularly sensitive (Bevanda, 2005: 307-338; Mujović-Zornić, 2012: 23-44). Such relationship is or should be one of mutual trust. A prerequisite for taking any medical action or treatment is a two-way communication, i.e. exchange of information between a doctor and a patient. The quality of healthcare and safety of patients depend to a large extent on their mutual communication and trust. If the doctor does not enjoy the patient's confidence and the patient does not rely on the doctor's expertise and professionalism, a medical service that doctor provides cannot be a safe and high-quality service. A doctor gets plenty of information on the patient's private life, which can be very important for diagnosis and medical treatment (La France, 1999: 509). In order to get a more efficient medical treatment, it is essential for patients to answer sincerely doctors' questions, thus providing complete and accurate information about their health, even the information that may be unpleasant or incriminating to patients or their family members. In this way, patients express their confidence in reliability, expertise and professionalism of their doctors.

Doctors are expected to provide medical services professionally and with care (i.e. with professional diligence). This implies their professional caution acquired through special professional education, improved by their practical experience and enhanced contemporary knowledge of medical science and the principles of legal practice in the field of medical law (Geisen, 1984: 16-17, as cited in: Radišić, 1986: 157). Patients and doctors are aware that doctors' professional behaviour and care include a special legal and moral obligation to protect the interests of patients. Doctors protect interests of patients by keeping the patients' privacy, or by keeping as a professional secret the information about patients that they learn while providing their patients' medical treatment. Protection of health-related personal data is particularly important for the right to respect the private life of a patient.

Unjustified and unlawful disclosure of personal health information constitutes a malpractice and unprofessional conduct of the medical staff. Such behaviour is a medical malpractice² that could cause a violation of material (property) and intangible (non-property) assets of the patient whose medical information is published. This results in civil liability.³ In Bosnia and Herzegovina law, civil liability of medical professionals, including doctors as relevant providers of

healthcare, for violation of the patients' rights to privacy and protection of personal health data is not regulated by special regulations, which would be valid only for healthcare professionals. Hence, it is determined by the general provisions on tort i.e. by the provisions of the Law on Obligations.⁴

1.2 Right to protection of personal data

Patient's right to privacy and confidentiality of their personal health data is one of the fundamental human and personal rights – the right to respect private life,⁵ which is regulated in all international and regional human rights documents.⁶

The affirmation and establishment of the right to respect private life have its roots in the protection of personal data (Dragičević, 2001: 619, 620). Numerous relevant cases before the European Court of Human Rights indicate that the right to protection of personal data is given the fundamental importance within the context of the right to private and family life.⁷

Specific legal acts that regulate this area have been adopted in Europe in order to effectively protect personal data.⁸ The Council of Europe has adopted the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data⁹ and Additional Protocol to the Convention.¹⁰

Reformation of the framework for the protection of personal data has been one of the largest and most complex challenges in the EU in recent years.¹¹ The digital single market is faced with numerous challenges of modern digital age that make the protection of fundamental rights to privacy and protection of personal data a very complex issue.¹² Therefore, a clear, strong and effective legal framework is essential for the protection of the fundamental rights to privacy and protection of personal data. It is at the same time a key constituent element of the digital single market.¹³

In the modern (digital) time, the protection of rights and fundamental freedoms of individuals with regard to the processing of their personal data is an important issue in many EU policies. The European Union has adopted several directives, including the most important one – Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.¹⁴ It is a basic legal instrument of the European legislature which seeks to harmonise the regulations of the Member States regarding the protection of personal data. This Directive is designed and made with two objectives: the first is the protection of individuals against unauthorised public exposure of their personal data, and the second is to ensure a free movement of personal data within the internal market.

Since the time of the adoption of the Directive 95/46/EC, the information and communication technology has developed rapidly. As a result, some of its

provisions have become inadequate and have not reached the desired degree of harmonisation of Member States' rights in this area. Therefore, the EU has recently adopted a new legal instrument, the General Data Protection Regulation (hereinafter: GDPR), regulating data protection framework across the EU in a modern and harmonised way, based on which the EU citizens benefit from facilitated procedures for access and protection of personal data.¹⁵ The GDPR repeals the Directive 95/46/EC with effect from 25 May 2018.

As stated in recital 9 of the GDPR, due to differences in the implementation and application of Directive 95/46/EC, the level of protection of the rights and freedoms of natural persons is different, in particular, the right to protection of personal data, with regard to the processing of personal data in the Member States. These differences may prevent the free flow of personal data throughout the Union and "may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law." GDPR was adopted in order to ensure a consistent level of protection for natural persons throughout the Union and to prevent differences that hinder the free movement of personal data within the internal market.¹⁶

The right to protection of personal data, as an important component of the right to private and family life, is regulated by the constitutions and other legal instruments in national legal systems. Some states have adopted special laws that regulate the protection of personal data, their collection, processing and use and special institutions have been established in order to control the processing of such data. Bosnia and Herzegovina is among these states. It is a party to the Convention no. 108,¹⁷ and as a potential candidate for membership in the EU,¹⁸ the state follows the framework for regulation of personal data protection adopted in the EU law while seeking to harmonise its legislation with the *acquis communautaire*.¹⁹ The European Union monitors the commitment of Bosnia and Herzegovina to promote democratic values, the rule of law and respect for human rights (including the right to protection of personal data) in accordance with Article 49 of the TEU²⁰ and provides guidance and support to achieve a tangible and sustained progress in the key areas of the reform.²¹

Bosnia and Herzegovina has adopted the Personal Data Protection Act in 2006 (hereinafter: PDPA).²² As a basic legal instrument in the area of personal data protection in the state, PDPA essentially reflects the provisions of Directive 95/46/EC.²³ The Agency for Protection of Personal Data (hereinafter: APPD) was established according to PDPA, which is in charge of supervising the processing of personal data in B&H.²⁴

The provisions of PDPA and the provisions of numerous laws of health and healthcare as standardised patient's right to privacy and confidentiality of

information about his health have been applied to the protection of personal data of the patient in the B&H legal system. Analysis of these provisions, as well as insight into the situation in practice, based on the APPD's report and available case law, will show the extent to which Bosnia and Herzegovina has respected the rights of patients and a level of potential divergence of its law compared to the regulations and standards in the EU Member States.

2 Legal regulation of protection of patient's personal data in Bosnia and Herzegovina

As mentioned above, health-related personal data are considered a special category of personal data.²⁵ The issue of protection of patient's personal data is governed in Bosnia and Herzegovina by the provisions of health and health care acts. Since the Federation of Bosnia and Herzegovina, Republika Srpska and the Brčko District of Bosnia and Herzegovina all have the jurisdiction to standardise this area, there is a multitude of laws governing it.²⁶ First, we should mention the laws on healthcare, because they could be characterised as a *lex generalis* in terms of patients' legal status. This primarily refers to Republika Srpska²⁷ and the Brčko District,²⁸ while in the Federation of B&H such is the function of the Law on Patients' Rights, Obligations and Responsibilities (hereinafter: LPROR).²⁹ Healthcare Act of the Federation of B&H (hereinafter: HCAFBH)³⁰ regulates patients' rights only in several provisions, referring further to the provisions of LPROR in terms of a more detailed regulation.³¹

2.1 Law on patient's rights, obligations and responsibilities of the federation of Bosnia and Herzegovina

LPROR guarantees to every patient³² the right to confidentiality of his personal information and privacy, and the right to keeping their data confidential. Under this law, the right to confidentiality of information includes all personal information that a patient has communicated to a relevant healthcare worker, including the information related to his/her state of health and potential diagnostic and therapeutic procedures. It extends to the period after the patient's death.³³ Relevant healthcare worker is explicitly forbidden from sharing the patient's personal information with other people.³⁴ The exception to this rule concerns the death of a patient when the patient's right to access to medical files is exercised by his successors. They are entitled to obtain information from medical records that are related to the cause of death and medical procedures prior to his death.³⁵ LPROR regulates the patient's right to appoint a close family member to be informed about his/her disease and proposed medical treatment in case he/she refuses to receive the information needed to give an informed consent.³⁶ If the patient fails to determine that person, the doctor is entitled to give a notice of the patient's health status to an adult member of the immediate family who shares the same household with the patient, in case it is necessary so as to avoid health risks for other household members.³⁷

The right to patient's privacy is guaranteed during the implementation of diagnostic tests, visits to a doctor or a dentist or specialists as well as the entire medical-surgical treatment. LPROR explicitly provides that only health workers and medical staff may be involved in the treatment. The patient may exceptionally request the presence of the members of his/her family or the persons of his/her choosing during the examination and medical procedures. When it comes to children under 15 or a person deprived of legal capacity, the presence of their legal representative is required.³⁸ In order to achieve greater protection of patient's privacy, LPROR standardises an obligation of health institutions and health professionals to ensure the audio and visual privacy of patients during the medical procedures, except in a case of emergency.³⁹

The right to confidentiality is regulated in detail by LPROR. The law stipulates that data from medical records belong to the patient's personal data and constitute a professional secret.⁴⁰ To protect such secrets is the obligation of health professionals, health associates and other persons employed in health institutions, private practice, or the Health Insurance Fund in which the patient is secured, as well as authorised assessors of the external quality control in a medical institution or private practice. Apart from them, the duty of confidentiality is prescribed for people who participate in the preparation and publication of professional and scientific papers, marketing materials of medical institutions, as well as persons involved in teaching process at health institutions. All of the above-mentioned individuals may be exempted from the obligation to keep the confidentiality of data only by a clear and unambiguous patient's consent or when these obligations are exempt under the provisions of criminal procedure and civil procedure legislation.⁴¹ The patient's right to confidentiality of personal data is quite widely defined in LPROR since it entails his/her right to allow the use of such information after his/her death only to persons designated by him-/herself. If this right is not consumed, as stated above, the right of access to his personal information will only belong to his heirs, as exhaustively defined by law.⁴²

2.2 Laws on healthcare in Republika Srpska and Bračko District of Bosnia and Herzegovina

In accordance with the provisions of HCAFB&H and LPROR, the laws on healthcare in Republika Srpska and Brčko District standardise in detail the rights and duties of citizens and patients in the healthcare system.⁴³ Among these rights are the patient's right to confidentiality of personal information that he/she gives to his/her doctor,⁴⁴ the right to protection of his/her privacy during diagnostic tests, specialist visits and medical-surgical treatment in general⁴⁵ as well as the right of access to his/her own medical records.⁴⁶ These rights have been standardised almost identically as in HCARS and HCABD. Comparison of these provisions with relevant provisions of LPROR shows certain differences,⁴⁷ but the general assessment is that they are mutually compatible to a significant extent.

The provisions directly or indirectly related to patients' rights to protection of personal data can be found in the law on health insurance,⁴⁸ laws on the health care records,⁴⁹ laws on rights and obligations of medical professionals in the exercise of their profession,⁵⁰ as well as certain subordinate legislation in the field of health and healthcare, applicable to both BH entities and Brčko District. In addition to these acts, the patient's right to protection of personal data is directly or indirectly sanctioned by the laws that regulate special areas of healthcare or special medical procedures, such as the protection of persons with mental disorders,⁵¹ abortion,⁵² organ and tissue transplantation,⁵³ blood transfusion⁵⁴ etc.

3 The state and perspective of protection of personal data in Bosnia and Herzegovina

3.1 Reports of the Agency for Protection of Personal Data

Insight into the reports on the protection of personal data, which the Agency for Protection of Personal Data in Bosnia and Herzegovina annually submits to the Parliamentary Assembly of Bosnia and Herzegovina, shows that some progress has been made in this field. Thus, in the report from 2012, the APPD stated that the situation in the field of protection of personal data did not reach a satisfactory level, either in formal or factual terms. In particular, it pointed to the fact that the inspection controls implemented by the APPD found an unacceptable situation (lack of regulations, the absence of rules and procedures, lack of plans for the protection of personal data) in most of the monitored institutions. The Agency has conducted 34 regular inspections of the controllers⁵⁵ – health institutions from all over B&H - and noted the same or similar deficiencies related to establishing and maintaining records of personal data in accordance with the relevant legislation, keeping medical records and providing information about patients' health to the third parties contrary to the current regulations, etc.⁵⁶

Inspection controls on the processing of personal data in practice that the APPD did in public and private health institutions in 2013⁵⁷ revealed the same shortcomings as in the previous period. Apart from that, an analysis of legislation in the field of health was done and it pointed to the shortcomings in certain laws and their practical implementation, which violated patients' right to confidentiality of information about their health.⁵⁸

In the report on the protection of personal data for 2014, the APPD gave a general assessment that B&H formally complied with European standards and that the situation in that field was satisfactory. When it comes to the protection of health-related personal data, the Agency stated that it received seven complaints in 2014.⁵⁹

In the eighth report on personal data protection in Bosnia and Herzegovina, the one from 2016, the APPD stresses its dissatisfaction with the situation in the field of personal data protection in B&H in both formal and factual sense. However, the

agency "expressed satisfaction with the progress that was made in the field of personal data protection in Bosnia and Herzegovina in 2015".⁶⁰ In the reporting period, out of 19 ex officio procedures against public authorities, one trial was conducted against the controller who collected the medical records of the insured people from their employers⁶¹ and against one controller for conducting audio surveillance in pharmacies.⁶²

In total, 57 complaints have been filed with the APPD against the controllers from the private sector, four of which related to the processing of data on health status.⁶³

3.2 Opinion of the future European Commission

Unlike the relatively positive opinion of the APPD with regard to the situation in the field of personal data protection in Bosnia and Herzegovina, the European Commission, in the Report on the progress of Bosnia and Herzegovina in 2015, took the view that B&H has achieved only partial compliance with European standards in this field.⁶⁴ The same assessment by the European Commission was presented in the Progress Report of Bosnia and Herzegovina in 2016.⁶⁵

There are many indicators that the effective implementation of adopted legislation on the protection of personal data is not satisfactory, which suggests that the area of personal data protection in B&H is still far from the high formal level of alignment with the acquis, in particular on the factual level.

3.3 Judgement of the Court of Bosnia and Herzegovina

Violation of the right to protection of personal health data is discussed in B&H jurisprudence. Thus, in a proceeding before the Court of Bosnia and Herzegovina, the merits of the APPD decision were assessed. This decision was passed on the appeal of an employee against her employer and health institutions, which, upon the employer's request, submitted personal information about the employee's health.⁶⁶ The APPD found that in this particular case, there was no violation of the right to data protection of the person who filed the complaint, because the "treatment of special categories of data needed to meet the obligations and special rights in the field of labor law," and their procedure treatment "was carried out legally, without violations of the provisions of the PDPA and the implementing regulations".⁶⁷ The employee then filed a suit against the APPD, challenging the above ruling. The Court of Bosnia and Herzegovina dismissed the claims of the plaintiff and held that the solution of the APPD is justified where the Agency correctly decided that the prosecutor's objection was unfounded. The Court of Bosnia and Herzegovina in the reasoning of its decision referred to the relevant case law of the European Court of Human Rights in connection with the disclosure of medical information (Z. against Finland - February 25, 1997). In addition, it emphasised "that the purpose and objective of the PDPA is not a universal ban on the use of personal data, but control

methods for their use and processing so as to avoid their diversion and thus ensure the protection of human rights and freedoms prescribed in art. 1 of the PDPA.⁶⁸

4 Conclusion

The right to respect privacy and protection of personal data is a fundamental right, which expresses common values and constitutional heritage of Europe.⁶⁹ Health-related personal data are considered a special category of data, and their protection is one of the fundamental rights of patients.

On its path to the EU membership, Bosnia and Herzegovina is gradually taking over the acquis of the Union in the field of protection of personal data, incorporating the provisions of the personal data protection modelled on the regulations of European law into its legal system.

Besides the PDPA, as a fundamental act and *lex generalis*, there are numerous regulations in the field of health and healthcare in B&H comprising the rules on the protection of patients' personal data. With regard to the distribution of legislative competence in this area, there is a number of multiple, but not quite uniform, legal sources. The complex organisation and financing of the healthcare system in the state with overwhelming corruption prevent the reaching of a higher level of health protection and the safety of patients.

These reasons, as well as many others, create a certain dose of legal uncertainty in practice. Patients do not have confidence in health institutions and health workers in terms of personal health data security and protection. This distrust is reflected in annual reports of the APPD, relevant case law and the annual reports of the European Commission on the progress of B&H.⁷⁰

The application of regulations for the protection of patients' rights to privacy and protection of personal data in Bosnia and Herzegovina should be far more effective than it is now. In order to achieve a high level of protection of natural persons, i.e. patients, in the future period, it is necessary to respond to new challenges in the protection of personal (health) information, the development of clear and solid legal and other frameworks that are harmonized with the EU's package of reforms in the area of data protection. However, a formal harmonisation of legislation will not mean anything to the citizens if they miss, as it has been so far, the practical implementation of effective regulations.

Notes

¹ Radolović points out that the contract on the medical treatment "... is not a simple legal relation. It covers four main parties: health insurance service, health institution (hospital) which carries out the treatment, doctors and other medical staff who, as employees of hospitals, directly implement treatment, and patient as users of their services. This legal relation includes further "complications". It contains, in fact, several private legal relations and then several private legal acts: the relationship between a health insurance service and a patient (insured), the relationship between health insurance service and health institutions (hospitals), the relationship between hospitals and doctors (and other medical staff) as well as the relationship between a patient and a hospital or its medical staff."(Radolović, 2014: 110).

² "Medical malpractice implies malpractice of doctors, nurses, pharmacists, medical therapists and other healthcare professionals who are responsible for the healthcare of patients and citizens", The Supreme Court of the Federation of Bosnia and Herzegovina No. 43 0 P 019379 13 Rev of 23. 03. 2015 (Domaća i strana sudska praksa, God. XII., Br. 64, 2015: 62); "Any medical malpractice does not mean *a priori* existence of the responsibility of doctors." The decision of the Dubrovnik County Court, No: 8 Gz-281/16 of 1 June 2016, <https://sudskapraksa.csp.vsrh.hr> (January 1, 2017).

³ Unauthorized intrusion into patients' privacy or unauthorized disclosure of their personal data can cause a violation of material (property) and intangible (non-property) assets of patients, which is a basis for civil liability. In addition to compensations, unauthorized disclosure of professional secret can produce other types of liability of doctors (medical professionals): criminal, misdemeanor and disciplinary. Since this question requires a separate detailed analysis, it will not be further discussed in this paper (Bevanda & Čolaković, 2016: 127, Crnić, 2009).

⁴ The Law on Obligations (published in the OG of SFRY no. 29/78, 39/85, 45/89, 57/89, coming into force on 1 October 1978) originates from the former Yugoslavian legal system (Decree promulgating the Law on Obligation, OG of B&H, no. 2/92), amended by Decree with the force of law on amendments the Law on Obligations (OG of B&H, no. 13/93). Those Regulations are confirmed as laws by the Assembly of the Republic of Bosnia and Herzegovina (Law on Ratification of the decrees with the force of law, OG of B&H, no. 13/94). The Federation of Bosnia and Herzegovina and the Republika Srpska enacted several amendments to it: OG of FB&H, no. 29/03 and 42/11; OG of RS, no. 17/93, 3/96, 39/03 and 74/04.

⁵ As Gavella points out, the right to privacy is the right of a person to enjoy (private) life separately and independently of other people. It allows patients to live their life according to their own discretion, to treat themselves and their life according to their own needs and desires and to exclude any unauthorised encroachment on it by other persons, public or public authorities (Gavella, 2000: 65).

⁶ To mention a few: The European Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe 1950 (hereinafter: ECHR), which in art. 8 sanctioned the right to respect private and family life, home and correspondence, and the EU Charter of Fundamental Rights 2002 (OJ 2010 / C 083/02, hereinafter: EU Charter). The EU Charter became legally binding on 1 December 2009. Pursuant to art. 6. c. 1 TEU, it has the same legal effect as contracts, i.e. it is a part of the primary law of the EU. Unlike the ECHR, which does not regulate specifically the right to protection of personal data, but it is guaranteed in terms of the protection of right to privacy under art. 8, in the EU Charter, this

right is regulated as an independent right (Art. 8), in relation to the right to respect private and family life, home and correspondence (Art. 7). Such differences should not be surprising, if one bears in mind that at the time when the ECHR was created, information and communication technologies were not at such a stage of development to make personal data easy and widely accessible for collection, storage, processing and possible abuse, as it was at the time of the EU Charter, and even more so today. Bosnia and Herzegovina ratified this Convention on 12 July 2002 (OG of B&H, no. 6/99), and simultaneously with it or later, all Additional Protocols to the Convention. Pursuant to art. II, para. 2 of the Constitution of Bosnia and Herzegovina, "the rights and freedoms set forth in the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocols shall be applied directly in Bosnia and Herzegovina and have priority over all other law."

⁷ See more on the positions of the European Court of Human Rights regarding the protection of personal data (Dragičević & Gumzej, 2014: 44-5).

⁸ Personal data include any information (such as name, address, date of birth, identity card number or passport number, e-mail address, information about the workplace, professional qualification, tax returns, information on bank accounts, salary, and so-called special categories of data – data on citizenship, national, ethnic or racial origin, political, religious, philosophical or other belief, health, genetic code, sexual orientation, biometric data, etc.) related to a natural person who can be identified, directly or indirectly, by reference to one or more of those data.

⁹ The Council of Europe CETS No. 108, 1981 (hereinafter: The Convention no. 108). This Convention is the first international instrument of a binding character, which protects a natural person of abuse that can occur during the collection and processing of their personal data. It also regulates a cross-border transfer of personal data and applies to the processing of personal data in both private and public sector. The Convention can be freely accessed, even for the countries that are not members of the Council of Europe and are not situated on the European continent. Thus, the Convention has been signed by Uruguay, Mauritius, Senegal, Morocco, Cape Verde and Tunisia. Convention no. 108 was adopted on 28 January 1981, the day the European Commission and the Member States of the Council of Europe marked the Day of protection of personal data.

¹⁰ The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data concerning supervisory authorities and trans-border data transfer, CETS no. 181, 2001. This Protocol contains provisions on cross-border data transfer to the states that are not members of the Convention no. 108 and regulates the establishment of an independent supervisory body.

¹¹ The European Data Protection Supervisor, Annual Report 2014 Luxembourg: Publications Office of the European Union, 2015, p. 5.

¹² See: <https://ec.europa.eu/digital-single-market/> (January 17, 2017).

¹³ https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-14_ePrivacy_ex_summ_HR.pdf.

¹⁴ SL L 1995 L 281 (hereinafter: Directive 95/46/EZ).

¹⁵ The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation hereinafter: GDPR) (Text with EEA relevance), OJ of the European Union L 119, of 4 May 2016, pp. 1-88. This Regulation came into force on the twentieth day after its publication in the Official Journal of the EU, and will be applied from 25 May 2018.

¹⁶ See the 9th and 13th recitals and art. 1 GDPR.

¹⁷The Convention and the Additional Protocol entered into force in Bosnia and Herzegovina on 1 July, 2006.

¹⁸Bosnia and Herzegovina lodged an application for membership in the European Union on 15 February 2016., See: www.europa.ba.

¹⁹Such a commitment of Bosnia and Herzegovina arises from Art. 70 of the Stabilisation and Association Agreement, signed between the European Communities and their Member States, on the one, and Bosnia and Herzegovina, on the other hand. The agreement was signed in Luxembourg on 16 June 2008 and entered into force on 1 June 2015. The Council of Ministers of Bosnia and Herzegovina decided to start with the process of harmonisation of B&H legislation with the *acquis communautaire* in its 66th session held on 28 July 2016 (OG of B&H, no. 75/16).

²⁰According to Art. 2 and 49 TFEU, the EU is founded on the values of respect for human dignity, liberty, democracy, equality, the rule of law and respect for human rights, including the rights of minorities. Such values are common to the Member States in a society of pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men. Any European state which respects these values and is committed to promote them, can apply for membership in the Union.

²¹CELEX%253A52015JC0016%253AHR%253ATXT.pdf

²²OG of B&H, no. 49/06, 76/11 and 89/11.

²³The objective of this Act is to ensure to all persons on the territory of B&H, regardless of their nationality or place of residence, protection of human rights and fundamental freedoms, especially the right to privacy with regard to the processing of their personal data.

²⁴The Agency for Protection of Personal Data in Bosnia and Herzegovina is an independent administrative organization, whose responsibilities include the following: monitoring the implementation of the provisions of PDPA and other laws on the processing of personal data; acting upon the complaints submitted by the data holder; submission of annual reports on personal data protection to the Parliamentary Assembly of Bosnia and Herzegovina; monitoring requirements for the protection of personal data by giving proposals for enacting or amending legislation concerning the processing of personal data, and giving opinion on proposed laws as well as taking care of fulfillment of data protection criteria arising from international agreements binding for Bosnia and Herzegovina. For Agency details see: <http://www.azlp.gov.ba> (February 13, 2016).

²⁵Art. 6 of the Convention no. 108 under a special category of data defines personal data revealing racial origin, political opinions, religious or other beliefs, personal data concerning health or sexual life, as well as data concerning criminal convictions, while in art. 8 of Directive 95/46/EC, the data on worker union membership is also added to this category. These data deserve special processing treatment, which means that they cannot be processed without the consent of the person they refer to, except in exceptional cases provided by law. GDPR (art. 9.1) regulates that health-related data fall within a special category of data whose processing is generally prohibited. According to Art. 4 (15) of GDPR, the concept of "health-related data" refers to personal data concerning the physical or mental health of a natural person, including the provision of health services, or providing information about patient's health status. The 35th recital of the Regulation states: "Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person; a number, symbol or a particular assigned to a natural person to uniquely identify the natural person for

health purposes; information derived from the testing or examination of a body part or bodily substance, including genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.”

²⁶All criminal laws in force on the territory of B&H contain crime of "unauthorized use of personal data". According to Art.149 of the Criminal Code of B&H (OG of B&H, no. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06,55/06, 32/07, 8/10, 47/14, 22/15 and 40/15) official or responsible person in the institutions of B&H who, without the consent of the individual and contrary to the conditions prescribed by law, collects, processes or uses their personal data, or uses such data contrary to the statutory purpose of their collection, shall be punished with a fine or imprisonment not exceeding six months.

²⁷Healthcare Act of Republika Srpska, OG of RS 106/09 and 44/15, hereinafter: HCARS.

²⁸Healthcare Act of the Brčko District of Bosnia and Herzegovina, OG of BD 38/11, 09/13, 27/14 and 3/15, hereinafter: HCABD.

²⁹OG of FB&H 40/10. Republika Srpska and the Brčko District have not yet adopted a specific law on the rights and responsibilities of patients.

³⁰Healthcare Act of the Federation of Bosnia and Herzegovina, OG of FB&H 46/10.

³¹HCAFBH lays down the basic principles of healthcare (Art. 21-25.) and standardises human rights and values

of every citizen in healthcare. It enumerates, among other things, the right to physical and mental integrity and security of his personality (Art. 26 para. 1). In addition, the Act explicitly lists the rights of patients, which include privacy and confidentiality of data (Art. 27 para.2). Art.29 stipulates that the rights, obligations and responsibilities of patients, as well as protection of their rights, shall be specified in detail in the special act on the rights, obligations and responsibilities of patients.

³²Patient, in terms of this Act, shall refer to any person, sick or healthy, insured or uninsured person, who requests or who is undergoing certain medical measures or services with the aim of preserving and improving health, preventing illness, treatment or medical care and rehabilitation (Art. 1 para. 3). The same definition of the patient can be found in HCAFBH (Art. 27 para. 1).

³³Art. 26 para. 1 LPROR.

³⁴Art. 25 LPROR. This provision may refer to an incomplete observation, because the prohibition of communicating patient data to other persons is imposed only for the relevant health professionals to whom the data were directly given by the patient. In theory and practice, this could be a situation where the patient's personal information is communicated by some other "non-authoritative" health professional, who has collected the information indirectly, by authorized or unauthorized insight into the medical records, or found it otherwise. Therefore, it would be better to have this ban cover all healthcare workers.

³⁵In addition to the right of access to medical record, patient's heirs have the right to receive its copies (Art. 36 LPROR).

³⁶Art. 13 para. 2 LPROR.

³⁷Art. 15 para. 3 LPROR.

³⁸LPROR uses the term "legal representative or guardian" in this (Art. 26 para. 3), but also in some other provisions which standardise the status of underage patients and patients deprived of legal capacity (see art. 22, para. 1 and 7). This solution is incorrect, because 'legal representative' is a common term for parents and custodians. Therefore, this error should be corrected.

³⁹Art. 26 para. 3 LPROR.

⁴⁰Art. 27 para. 1 LPROR. According to para. 2 of this Article, personal data includes all identification and identifying information about patient's health and medical condition, diagnosis, prognosis and treatment, and information about human substances based on which personal identity can be determined as well as remittances for sick leave which should be delivered to the employer in a sealed envelope.

⁴¹ Art. 28 LPROR. This article regulates that the persons who are under the obligation to maintain the confidentiality of data must perform their processing in accordance with PDPA.

⁴² These are, as follows, patient's marital/cohabitant partner, adult children, parents or adoptive parents (Art. 29 LPROR).

⁴³Art 17-34 HCARS; Art. 21-43 HCABD.

⁴⁴Art. 29. HCARS; Art. 37 HCABD. Both articles proclaim the right of a patient to give a relevant doctor a written consent to communicate their personal data to other persons. This may be one of the adult members of the patient's family. The doctor is authorized without such consent to inform the adult family member of the patient's state of health if this is necessary in order to avoid health risks for other family members.

⁴⁵Art 30 HCARS; Art. 38 HCABD.

⁴⁶Art 33 HCARS; Art. 41 HCABD.

⁴⁷It should be noted that patient's right to privacy and the obligation of medical professionals to maintain the confidentiality of patient data in HCARS and HCABD is not regulated in such detail as in LPROR. These two laws only standardise the patients' right to have access to their medical records and the equal right of the members of their immediate family, but only exceptionally, if such data are important for their health (Art. 33 HCARS; Art. 41 HCABD).

⁴⁸ Health Insurance Act of the Federation of Bosnia and Herzegovina, OG of FB&H 30/97, 02/07, 70/08 and 48/11; Health Insurance Act of the Republika Srpska, OG of RS18/99., 51/01, 70/01, 51/03, 57/03, 17/08, 01/09 and 106/09.; Health Insurance Act of the Brčko District of Bosnia and Herzegovina, OG of BD 1/02, 7/02, 19/07, 2/08and 34/08.

⁴⁹Health Care Records Act of the Federation of Bosnia and Herzegovina, OG of FB&H 37/12.; Health Care Records and Statistical Surveys Act of the Republika Srpska, OG of RS53/07. In the Brčko District of Bosnia and Herzegovina, such law has not yet been adopted.

⁵⁰ In the Federation of Bosnia and Herzegovina those are: Law on Medical Practice, OG of FB&H 56/13. Law on Nursing and Midwifery, OG of FB&H 43/13. Law on Dentistry, OG of FB&H 37/12. Law on pharmacy activities, OG of FB&H 40/10. The Republika Srpska has so far adopted only the Law on pharmaceutical activities, OG of RS119/08. and 1/12. These laws do not exist in Brčko District.

⁵¹ The Law on the Protection of Persons with Mental Disabilities of the Federation of Bosnia and Herzegovina, OG of FB&H 37/01., 40/02. and 52/11.; The Law on the Protection of Persons with Mental Disorders of the Republika Srpska, OG of RS46/04; The Law on the Protection of Persons with Mental Disorders of the Brčko District of Bosnia and Herzegovina, OG of BD 12/06.

⁵² Law on conditions and procedure for termination of pregnancy in Bosnia and Herzegovina, OG of B&H29/77. This law still applies in the Federation of Bosnia and Herzegovina and the Brčko District of Bosnia and Herzegovina. Several years ago, Republika Srpska adopted a new Law on conditions and procedures for termination of pregnancy, OG of RS 34/08.

⁵³Law on transplantation of human organs and tissues of the Federation of Bosnia and Herzegovina, OG of FB&H 75/09; Law on transplantation of human organs of Republika

Srpska OG of RS 14/10. Law on transplantation of human tissues and cells of Republika Srpska, OG of RS14/10.

⁵⁴Law on Blood and Blood Components of the Federation of Bosnia and Herzegovina, OG of FB&H 9/10; Law on transfusiology of the Republika Srpska, OG of RS 44/15. Brčko District of Bosnia and Herzegovina has not yet adopted such law.

⁵⁵Pursuant to Art. 3a PDPA, the controller is any public authority, natural or legal person, agency or any other body which alone or together with others conducts the processes and determines the purpose and means of processing personal data on the basis of law or other regulation.

⁵⁶Report on the Protection of Personal Data in Bosnia and Herzegovina for 2012, available at: <http://www.azlp.gov.ba> (January 13, 2017).

⁵⁷ There was a total of nine. Quoted from Report on Personal Data Protection in Bosnia and Herzegovina for 2013, available at: http://www.azlp.gov.ba/publikacije/Archive.aspx?langTag=bs-BA&template_id=149&pageIndex=1 (February 2, 2017).

⁵⁸For example, the practice of writing diagnosis codes in the certificate delivered to the employer to verify the temporary inability to work was observed and judged as unacceptable. According to the PDPA's opinion, it is enough for the employer to know how long the worker will be absent in order to plan the work. See *Ibid*.

⁵⁹One such objection was filed by an employee of Raiffeisen Bank dd B&H against the employer and the "Health Center Bihać" for checking information on her state of health. Although the employee regularly justified her absences through reports on temporary inability to work, the Bank requested additional information about her state of health from the Health Center, which was submitted to the Bank. The Bank stated that the mentioned information was necessary to acquire the knowledge or indications of the emergence of occupational diseases. The Agency determined that the Bank looked for disseminating information concerning the health status of an employee in the unauthorized manner and procedure, The Health Center violated the patient's rights to confidentiality of data and privacy. APPD states that in this case the processing of special categories of personal data was not necessary for the performance of obligations and specific rights of the controller in the field of labour law to the extent specified by law. Neither the Bank as an employer had the right to demand information from the Health Center on the type of disease (or whether it was occupational disease), nor the Health Center had a legal basis for the submission of this information. The Agency has concluded that this violated the right to privacy of the complainant. See: Report on the Protection of Personal Data in Bosnia and Herzegovina for 2014, available at: <http://www.azlp.gov.ba> (January 13, 2017).

⁶⁰Report on the Protection of Personal Data in Bosnia and Herzegovina for 2015, available at: <http://www.azlp.gov.ba>

⁶¹In the first case, the Health Insurance Institute of Sarajevo Canton, with a request for reimbursement of salary compensation during temporary inability to work more than 42 days from the employer to his employees, demanded an opinion of the doctor-specialist and a medical board. PDPA in its Decision (against which the Institute filed a complaint before the Court of Bosnia and Herzegovina) said that the demand of the Health Insurance Institute exceeds the necessary measure and the volume of the processing of personal data, since the calculation of salary compensation and reimbursement of wages can be made on the basis of remittances. Therefore, the Institute is prohibited from collecting other medical documentation, except remittances, and ordered to destroy collected documentation. *Ibid*.

⁶²In the second case, in the procedure which the Agency conducted *ex officio*, it was found that ZU 'My Pharmacy' for the purposes of personal and property safety in stores, carried out

the processing of personal data via audio surveillance, (recording the voice of employees and patients). ZU 'My Pharmacy' was prevented by the APPD to conduct audio surveillance in its shops and ordered to erase the created recordings. Ibid.

⁶³Such, for example, is a client complaint against a private surgical clinic in Sarajevo, submitted for processing data on medical treatment in the Commission's opinion of this institution, which was later delivered to the cantonal sanitary inspector. The complaint was adopted as established and the clinic was ordered to erase the data on the health status of complainant in the present Opinion, so that further actions are not available and visible. Ibid.

⁶⁴The above report is available on the official website of the Directorate for European Integration of Bosnia and Herzegovina: <http://www.dei.gov.ba> (January 16, 2017).

⁶⁵The report is available at: <http://www.dei.gov.ba> (January 17, 2017).

⁶⁶http://www.azlp.gov.ba/upravni_sporovi/P9.pdf

⁶⁷The request of the employer was sent to the Clinical Institute of Occupational Health and Sports of the Republika Srpska and Health Centre Banja Luka to provide the information on the health state of one of his employees (whether she is on sick leave and for how long) on the basis of her medical records, in order to plan and organize the work process. Health institutions have provided data on codes of disease, the first day of the inability to work and the completion day of sick leave, but have not provided the information on the diagnosis of disease, health status or content of medical records, as well as data that belong to a special category of personal data.

⁶⁸Judgement of the Court of Bosnia and Herzegovina no. S1 3 U 01015612 U, February 26, 2014.

⁶⁹The European Commission, Press Release, Fundamental rights: EU Charter is gaining more importance, to the benefit of citizens, Brussels, April 14, 2014.

⁷⁰In Bosnia and Herzegovina, there is a need for significant improvement of legal and factual framework of respecting patients' rights to privacy and protection of personal data, which is evident from the Communication of European Commission's enlargement policy for 2016 stating that in B&H "still exists the need for substantial improvement of strategic, legal, institutional and policy framework for the respect of human rights. Corruption remains prevalent in many areas and continues to be a serious problem. Declarative political commitment to this issue is not translated into concrete results." See: Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions, a Communication on the enlargement policy for 2016, Brussels, 09.11.2016, COM (2016) 715 final.

References

Bevanda, M. (2005) Ugovor između liječnika i pacijenta, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 26(1), pp. 307-338.

Bevanda, M. & Čolaković, M. (2016) Pravni okvir za zaštitu osobnih podataka (u vezi sa zdravljem) u pravu Europske unije, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 37(1), pp. 125-154.

Crnić, I. (2009) *Odgovornost liječnika za štetu* (Zagreb: Organizator).

Donev, D. (2013) Etički aspekti suvremenog modela odnosa liječnik – pacijent, *European Journal of Bioethics JAHR*, 4(7), pp. 503-512.

Dragičević, D. (2001) Privatnost u virtualnom svijetu, *Zbornik Pravnog fakulteta u Zagrebu*, 51(3-4), pp. 615-664.

Dragičević, D. & Gumzej, N. (2014) Obvezno zadržavanje podataka i privatnosti, *Zbornik Pravnog fakulteta u Zagrebu*, 64(1), pp. 39-80.

Gavella, N. (2000) *Osobna prava* (Zagreb: Pravni fakultet Sveučilišta u Zagrebu).

La France, A. (1999) *Bioethics: Health Care, Human Rights and the Law* (Newark: Lexis Nexis).

Mujović-Zornić, H. (2012) Odnos lekara i pacijenta kao etički i pravni odnos iz ugovora o lečenju, In: *Zbornik radova Medicina i pravo II* (Mostar: Medicinski fakultet), pp. 23-44

Petrić, S. (2012) Odštetna odgovornost zdravstvenih ustanova i djelatnika, In: *Zbornik radova Medicina i pravo II* (Mostar: Medicinski fakultet), pp. 46-78

Radišić, J. (1986) *Profesionalna odgovornost medicinskih poslenika* (Beograd: Institut društvenih nauka).

Radolović, A. (2014) Pravni poslovi prava osobnosti, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 35(1), pp. 95-108.

