Biuletyn Stowarzyszenia Absolwentów i Przyjaciół Wydziału Prawa Katolickiego Uniwersytetu Lubelskiego t. XIV, 16 (2) 2019, s. 87-100
https://doi.org/10.32084/sawp.2019.14.2-6

Edyta Marciniak

PROTECTION OF HEALTH DATA IN ACCORDANCE WITH THE GDPR: SELECTED ISSUES

Patient's rights are ranked among human rights. They are inalienable and rested upon human dignity. Human dignity also underlies other values, such as protection of life and health, and underpins the establishment of human rights. It has been acknowledged by the Supreme Court as one of the key personal interests. As the court put it in its 25 April 1989 decision, "personal dignity is that sphere of personality which is reflected in person's self-esteem and expectation of respect from others."[1] Access to information, especially about yourself, signifies social and legal awareness. In contrast, any limitations thereto result in deprivation of the right to self-determination as well as of the possibility of satisfying one of the most essential human needs, so important in the modern world. However, the processing of person's data cannot be avoided in contemporary reality. It is indispensable for the proper operation of the society and, admittedly, benefits each individual. For the processing of our data makes us part of the social, economic, or political life.

The opening part of the article attempts to define the concept of health data, primarily against the backdrop of 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 (General Data Protection Regulation)*,[2] as well as explaining the concept of genetic and biometric data and the overlap and approximation of all these

EDYTA MARCINIAK, Ph.D. student in the Department of Public Economic Law, Institute of Law, Faculty of Law, Canon Law and Administration, the John Paul II Catholic University of Lublin; Al. Racławickie 14, 20-950 Lublin, Poland; e-mail: solecka.edytka@gmail.com; https://orcid.org/0000-0002-0152-3802

[1] I CR 143/89, OSPiKA 9 (1990), item 330.

[2] Official Journal of the European Union L 119/1 with adjustment [henceforth cited as: GDPR].

definitions. The next part covers the safeguarding of personal data due to medical privacy, in accordance with the GDPR, against unauthorized access. The author addresses the obligations of physicians running individual clinics and of major healthcare facilities, which implement measures to ensure patients' full anonymity. The closing part of the article is devoted to the consent of the rightsholder to the processing of health data, how it is given and withdrawn, as well as to the question of consent by a person under 18 years of age.

1. The concept of health data

The right to the protection of health data (also personal medical data) is a liberty right vested in every person, regardless of their conduct and actions. It appertains the person throughout their life, and nobody can deprive them of it [Jackowski 2011, 27]. It is an inherent and inalienable right. Legitimacy of the right to the protection of health data is upheld by a number international instruments, just to mention the *European Convention on Human Rights*[3] (Art. 1), the *International Covenant on Civil and Political Rights*[4] (Art. 2), and the *United Nations Charter*[5] (Art. 1, para. 3). Because of being a human being, everyone is a holder of this right, regardless of whether they are even aware of it, or whether they accept and exercise it. The right to the protection of health data is associated with the idea of 'sensitive data'. Such information is among the most protected personal data. With the advancement of modern medicine, new challenges are emerging for medical scientists as well as for those pursuing various health professions. The use of ever newer and more innovative treatment approaches forces the medical industry and the academia to cooperate with a view to ensuring the protection of person's autonomy. At the same time, the existing laws cannot, despite restrictions resulting from the protection of personal privacy, impede a free data flow. As regards health data, special safeguards must be put in place to prevent health-based discrimination. Cases of employers or insurers who do not want to employ or insure sick

[3] Journal of Laws of 1993, No. 61, item 284.

[4] Journal of Laws of 1977, No. 38, item 167.

[5] Journal of Laws of 1947, No. 23, item 90.

people because of the financial risk involved are just an example to illustrate the point. For such entities, data on a person's health status is very valuable. Also, the progressing studies of the human genome may prospectively enable medical professionals to predict the future condition of a human being in the prenatal phase, that is, tell whether he or she will be susceptible to addictions or certain diseases. Consequently, given the above, if there were no strict protection of health data in the modern world, the person concerned would not be able to find employment or get insured and even, in extreme cases, socialize with others [Jackowski 2018, 25].

27 April 2016 saw adoption of GDPR which introduced a coherent system of personal data protection across the European Union. The main rationale for the revised data protection law was the accelerating integration between the EU member states and, by extension, the increasing transfer of personal data. An additional argument for the reform was the fast development of technology and spread of digitization, also having a major impact on everyday life. The GDPR fails to offer any definition of medical data. Yet, Art. 4(15) contains a definition of 'data concerning health', i.e. personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. As it says in Recital 35 GDPR, personal data concerning health 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 category includes information derived from the testing or examination of a body part or bodily substance, including (this may differ depending on the domestic law) from 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. Sensitive data also includes numbers, symbols or markings assigned to a natural person to uniquely identify the natural person for health purposes, such markings being given during the provision of medical services or already at the time of registration of the patient.

Also, the genetic and biometric data is defined in the GDPR. In accordance with Art. 4(13) GDPR, genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. On the other hand, biometric data, as defined in Art. 4(14) GDPR, means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. Attention should be paid to Recital 51 GDPR which emphasizes that data in question fall into a special category, which necessitates its processing using special technical means that allow the unique identification or authentication of a natural person. Whenever this data is not processed as indicated above, it cannot be qualified as biometric data.

What follows, genetic data can reveal information about person's health while being medical data at the same time; on the other hand, it can only concern the physiology of the person and his or her health status. An example of this is the data about somebody's height or hair colour. Similarly, biometric data can reveal the health status but may often be regarded as insignificant when determining the health condition of a person. It naturally follows that the concepts of health data, genetic data, and biometric data are complementary. In most cases, however, it is genetic data that, as opposed to biometric data, will be classified as health data [ibidem, 41]. It should also be stressed that, according to the case-law of the Court of Justice of the European Union, 'data concerning health' as defined in the GDPR, is a broader concept than 'health data'.[6]

2. Ensuring the security of health data processing

Each of us: present and future patients of various medical facilities, clinics or hospitals, may ask themselves a question: Is every entity

[6] Judgement of the European Court of Justice of 6 November 2003, file ref. C-101/01, Lex no. 192425.

providing health services obliged to respect the GDPR? The answer seems obvious, both from the objective and subjective (personal) perspective. For every healthcare establishment processes patients' data concerning health (as defined in the GDPR recitals). Within Art. 4(2) GDPR, processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. From the subjective perspective, there are two actors in this process: the processor and the patient or the so-called data subject. It is worth noting that the GDPR does not apply to the processing of personal data for personal purposes, for example, when medical records are collected and kept at home.

Healthcare facilities in the EU member states are bound by the GDPR as from 25 May 2018. The regulation does not point to any specific technical and organizational measures that the controller should employ to ensure effective data protection. These measures are to correspond to the scope, purpose and risk of a breach of processed personal data. Art. 32 GDPR offers examples of such technical and organizational measures that can be used to ensure adequate safeguards. These are: 1) pseudonymisation and encryption of personal data; 2) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; 3) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; 4) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Decisions to employ a specific security measure should be made taking into account the value of the processed data and the cost of its implementation but also the nature, scope, context and purpose of the processing, as well as any consequences of a data breach, for example, through its unauthorized disclosure or modification. Health data falls into such a data category whose processing requires the adoption of special security measures. In the case of data concerning health, differences in the

processing will also depend on the location. A physician running his or her own clinic usually has one electronic device to collect data about patients. On the other hand, in hospitals each doctor's computer is probably connected to a patient registration system that stores all medical records. All medical doctors employed in the facility can access it.

In view of the above, a system designed to process patients' personal data should be adjusted to the size and complexity of the specific medical facility. Access to medical records should be basically limited to authorized persons. Art. 9 GDPR seems to confirm that as it prohibits the processing of health data unless it is necessary for the purposes of preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of European Union or domestic law or pursuant to contract with a health professional. Moreover, personal data referred to in the previous sentence may be processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or domestic law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under European Union or domestic law. The prohibition to process health data laid down in Art. 9 GDPR has two forms, depending on specific data. The prohibition based on the objective criterion applies to data revealing racial or ethnic origin, political views, religious and ideological beliefs, trade union membership, genetic data, data concerning health, sex life and sexual orientation. Accordingly, if a piece of information provides a characteristic of one of the areas listed above, it cannot, in principle, be processed. In addition, there is a prohibition on the processing of data defined based on the subjective criterion and linked to the criterion of purpose of the processing, i.e. biometric data. It is not allowed to process this data if its purpose is to uniquely identify a natural person. For biometric data is personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person. To treat certain data as biometric data, it must meet all of the above conditions simultaneously. Biometric data must be subject to special technical processing, must relate to specific characteristics of a natural person and must enable the unique identification of a person. Failure to meet at least

one of these conditions excludes this data from falling into the biometric category. In addition, there is a category of biometric data that, according to the GDPR, is not data concerning health but, like other biometric data, is of great importance in diagnosis, treatment, assessment and comparison of human organisms. An example of this is anthropometric data gathered when conducting research among the population. This kind of data is processed and enable the identification of a natural person, but the processing is not done for this purpose. If this is the case, such data is relevant for medicine and does enable the identification of natural persons, however, is not treated as sensitive [Jackowski 2018, 128].

The GDPR also imposes certain obligations on physicians. They are attributed to medical confidentiality that binds healthcare professionals who are responsible for the processing of their patients' health data. Medical facilities should implement a number of measures to safeguard patients' data. Such measures are an antivirus system, anti-intrusion systems, password-protected hardware, storage of medical records in lockable cabinets and keeping doctors' offices closed [Koenner 2018, 22]. A very important document is the IT system management manual which describes actions and measures related to the security of computer programs, information on password policy (including password changes), logging in and out of the system, anti-intrusion or antivirus security, as well as backups. Such policies are vital because in the face of extensive digitization there is a risk that health data stored on electronic devices will be transferred to the public domain. The risk of violations resulting from unauthorized access to personal data should always be strictly controlled, and adequate response should be triggered. Physicians running clinics should equip their computers with antivirus and anti-spam applications. Medical staff should also be trained because even allowing a patient or stranger at the reception desk to peep at an active computer screen on for a short moment is likely to cause an unwanted leak of patients' data. The owner of a clinic as the controller of personal data and information security administrator is obliged to be familiar with the best and latest safeguards available on the market and instruct his or her personnel how to handle data. Patients' personal data is very much desired by banks, insurance companies and other institutions that are ready to pay a lot for getting hold of it.

Because patients' data is subject to strict protection, and medical facilities are required to implement measures to guarantee full patients' anonymity, a controversial solution adopted in the village of Wohyń, the Lublin region, in September 2018 deserves a special mention here. Patients were scheduled to visit the doctor's office by nicknames assigned to specific hours. So, instead of hearing their full name being called in the corridor, each patient was nicknamed and scheduled for a specific time of appointment. The list of the nicknames with assigned appointment times was posted on the clinic wall. Such an approach is a response to the complex and demanding requirements of the GDPR. Each patient's data should be completely secure, and nobody can find out what the person is treated for and by whom because the patient has the right to be completely anonymous. The provisions on the protection of health data do not point to specific security measures that should be put in place in outpatient clinics or hospitals, but they allow these establishments to decide independently what methods will be used to protect their patients' privacy. Despite numerous rules and restrictions imposed by the obligation to introduce special safeguards for health data, this solution offers some freedom to those who implement it. However, instead or making up and using nicknames to make appointments with patients, plain numbers would also suffice.

3. Consent of the rightsholder to health data processing

Art. 9(1) GDPR prohibits the processing of special categories of personal data. This data set includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning sex life or sexual orientation. However, exceptions to this prohibition do exist: they are listed in Art. 9(2) GDPR. Given that, the processing of health data is allowed, yet the purposes of the processing are limited to those expressly set out in the relevant regulations. Consent of the rightsholder is an extra condition for admissibility of health data processing, consent being defined in Art. 4(11) GDPR as any freely given, specific, informed and unambiguous indication of the data subject's wishes

by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The rightsholder's will can therefore be manifested in two ways: as an oral statement or clear action. The aforesaid affirmative action must be unambiguous.[7] Therefore, any activity aimed at processing health data, and covered by the requirement of the rightsholder's consent, should be based on the rightsholder's clear and active consent. Implied consent is not allowed; also, the lack of the rightsholder's objection or failure to make a statement to the contrary are not considered properly given consent. The request for consent to the processing of health data should be clearly separated from other business, as in the case of an electronically completed form where the consent to the provision of electronic services is required. Art. 7 GDPR supports this point by saying that the request for consent should be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Recital 32 GDPR mentions both a written (including electronic) and oral statement, hence Art. 7(2) GDPR will apply to all forms of consent: it can be the checking of a box on the website, selection of technical settings for using the services of the information society, or another statement or behaviour that indicates, clearly and in a specific context, that the data subject has accepted the proposed processing of his or her personal data, as provided in Recital 32 GDPR.

Withdrawal of consent is regulated in Art. 7(3) GDPR which says that the data subject has the right to withdraw his or her consent at any time. The withdrawal does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject should be informed about it. Consequently, it is the responsibility of the controller, i.e. the clinic or hospital, to inform the patient fairly (i) that the processing of health data does not affect his or her treatment, (ii) what are the effects of refusing consent, and (iii) that they can withdraw their consent at any time and without providing a reason. The withdrawal of consent should also be as easy as giving consent. The GDPR does not absolutely prohibit the performance of an agreement without one party's

[7] Art. 2 of Opinion 15/2011 of the Working Party of 13.07.2011, p. 21-23, http://www.archiwum.giodo.gov.pl/pl/1520110/4214 [accessed: 13.09.2019].

consent to process their personal data. By extension, a situation where, when concluding an agreement, the controller does not inform the other party that it will be necessary for the performance of the agreement to process his or her data cannot be ruled out. An example can be a beauty parlour that performs non-medical procedures, but after concluding an agreement with the client, he or she is required to provide his or her health data in order to carry on with a specific procedure [Jackowski 2018, 132]. This is in line with the principle of transparency laid down in Art. 5(1)(a) GDPR, the principle of transparency as well as the principle of balance between the data subject and the controller introduced in Recital 43 GDPR. However, the phenomenon outlined above causes the principle of balance to be compromised. Consequently, in such situations, the patient feels compelled to give consent in order to be able to benefit from some of the services. This destroys the very essence of consent which should be voluntary in the first place.

Speaking of the question of making the conclusion and performance of an agreement contingent upon the person's consent to the processing of their data, the link between the aforesaid provision and the principle of lawfulness contained in Art. 6(1)(b) GDPR must be explained. Data processing is in fact lawful when it is necessary to perform an agreement with the data subject as a party or to take action at the request of the data subject prior to concluding the agreement. What follows, in the case of data processing for the purpose of performing an agreement, the consent of the rightsholder to process his or her data seems not to be required. However, this does not apply to health data where the obligatory performance of an agreement does not determine the lawfulness of the processing of sensitive data, unless there is another condition met that makes the processing lawful, for example, an agreement has been concluded for the provision of medical services [ibidem, 133].

In accordance with Art. 9(2)(a) GDPR, consent to the processing of sensitive data must be explicit. Accordingly, it is not sufficient to consent only by making a confirmation: a statement must be given in writing, documented or even implied, still it must be an action clearly indicating that the person consents to the processing of his or her data. The request for consent should be clear and understandable as well as divided in terms of

the individual purposes of personal data processing. It is worth noting Art. 5(1)(b) GDPR which says that personal data must be collected for specified, explicit and legitimate purposes. So, before a person consents to the processing of their data, they must be made familiar with the purposes of the processing. Therefore, the principle of limiting the purpose of processing introduced by the above-mentioned article means that it is not allowed to express the said purpose too generally.

Conclusion

In order to secure medical data while observing the requirement to keep it confidential, it should be ensured that only authorized persons can have access to it. Some scope of health data must be accessed by a physician providing medical services to a patient, and some other by a nurse or a receptionist working in a healthcare facility. Two principles must be followed in this respect: the principle of minimized access and the principle of purpose. The scope of access to patient data should be kept to a minimum but should be sufficient to achieve the purpose of the processing and focused on that purpose. The controller should provide sufficient guarantees of implementing specific technical and organizational measures so that the processing meets the requirements of the GDPR and safeguards the rights of data subjects. It is also the controller's responsibility to adapt their forms, messages, e-mails or other queries to make them plain, clear and legible for the average recipient. They should also contain all the information necessary for the patient to give his or her consent to the processing after being informed in an explicit manner. For the quality of the information provided in the request for consent is relevant and not their size.

Analysis of the consequences of violating the right to have your health data protected and the question of giving and withdrawing consent to the processing may perhaps help this right to rise in importance among the public, and, as a consequence, ensure full protection of patient's privacy and autonomy of information. The EU legislator is introducing many new solutions in order to set behavioural patterns and interpretations unknown in previous regulations. Since entry into force of the GDPR, new procedures have emerged to secure the rights of data subjects. However, it

should be stressed that the existing literary output and case-law, as well as any past experience in the application of provisions ensuring the full rights of data subjects, are not ignored.

REFERENCES

Fischer, Bogdan, and Marlena Sakowska-Baryła. 2017. *Realizacja praw osób, których dane dotyczą, na podstawie rodo*. Wrocław: Biblioteka ABI Expert.

Jackowski, Michał. 2011. *Ochrona danych medycznych*. Warszawa: ABC.

Jackowski, Michał. 2018. *Ochrona danych medycznych. RODO w ochronie zdrowia*. Warszawa: Wolters Kluwer Polska.

Koenner, Marek. 2018. *RODO dla lekarza i podmiotu leczniczego w pytaniach i odpowiedziach*. Gdańsk: AsteriaMed.

Kubiak, Rafał. 2015. *Tajemnica medyczna*. Warszawa: Wydawnictwo C.H. Beck.

Protection of Health Data in Accordance with the GDPR: Selected Issues

Summary

Patients' rights are widely commented issue in the medical and legal press. Attempts are being made to analyse issues relating to patient consent, the right to information about the medical procedures performed and the state of health, or the authority of medical personnel to make decisions about the patient's person and the related procedures or treatments. This results in an increase in the importance of information, which has become one of the most important values in today's world. Access to information, especially about oneself, means a certain social and legal awareness. Restrictions on access to information deprive people of the right to self-determination and, at the same time, the right to satisfy one of their needs, which is particularly important in today's world. Nowadays, it is unavoidable to process the data of any person, which is essential for the proper functioning of society, but above all for the benefit of each individual. This testifies that an individual is present in social, economic or political life.

For over a year now, institutions providing medical services have been obliged to implement a number of regulations contained in the Regulation of the Parliament and Council 2016/679 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*. Personal data relating to health are defined in the preamble of the Act. This Regulation does not indicate the organisational or technical measures to be taken by the data administrator to ensure data protection. These measures should be appropriate to the scope, purpose and risks of the data being processed. Sensitive data shall fall within the category of data for which processing involves the adoption of enhanced security measures. The task of the

data administrator is to introduce appropriate guarantees to ensure the implementation of appropriate technical and organizational measures so that the data processing meets the requirements of the GDPR and protects the rights of data subjects. Their task is also to adapt their forms, statements, e-mails or other queries so that they are clear, understandable and readable for the average recipient. For it is the quality that is the essence of information provided in the inquiry, not its number.

The EU legislator has introduced several new developments to identify patterns of conduct and interpretations that are new concerning previous regulations. With the introduction of the GDPR, new procedures have been developed in order to exercise the rights of data subjects. However, the existing acquis of literature and judicature, as well as experience in the application of provisions ensuring the full entitlement of the data subjects, is not underestimated. More and more frequent analysis of the consequences of breaching the right to the protection of medical data and of the issue of giving and withdrawing consent to the processing of data may increase the importance of this right for society and thus ensure full protection of privacy and the information autonomy of the patient.

Key words: medical data, genetic data, biometric data, patient's rights, physician-patient privilege

Ochrona medycznych danych osobowych zgodnie z RODO. Zagadnienia wybrane

Streszczenie

Prawa pacjenta to zagadnienie szeroko komentowane na łamach prasy medycznej, jak i prawniczej. Podejmowane są próby analizy kwestii dotyczących zgody pacjenta, prawa do uzyskania informacji o wykonywanych zabiegach medycznych i stanie zdrowia czy uprawnień personelu medycznego do podejmowania decyzji dotyczących osoby pacjenta i związanych z nim zabiegów czy leczenia. Wynika z tego wzrost wagi znaczenia informacji, która we współczesnym świecie stała się jedną z najważniejszych wartości. Dostęp do informacji, szczególnie o sobie samym, oznacza pewną świadomość społeczną I prawną. Ograniczenia związane z dostępem do informacji powodują pozbawienie prawa do samodecydowania o sobie, a zarazem możliwości zaspokajania jednej z potrzeb człowieka, szczególnie ważnej we współczesnym świecie. Obecnie nie można uniknąć przetwarzania danych jakiejkolwiek osoby – jest to niezbędne dla prawidłowego funkcjonowania społeczeństwa, ale przede wszystkim jest z korzyścią dla każdego z osobna. Świadczy to bowiem obecności jednostki w życiu społecznym, ekonomicznym lub politycznym.

Od ponad roku placówki udzielające świadczeń medycznych mają obowiązek wdrażać szereg regulacji zawartych w Rozporządzeniu Parlamentu i Rady 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku*

z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Dane osobowe dotyczące zdrowia zdefiniowane zostały już w preambule tego aktu. Rozporządzenie nie wskazuje środków organizacyjnych ani technicznych, jakie administrator danych powinien stosować dla zapewnienia ochrony danych. Środki te powinny być odpowiednie do zakresu i celu oraz ryzyka naruszeń przetwarzanych danych. Dane wrażliwe zaliczają się do kategorii danych, których przetwarzanie wiąże się z przyjęciem środków wzmożonego bezpieczeństwa. Zadaniem administratora danych jest wprowadzenie odpowiednich gwarancji, zapewniających wdrożenie odpowiednich środków technicznych i organizacyjnych tak, aby przetwarzanie danych spełniało wymogi zawarte w RODO oraz chroniło prawa osób, których dane dotyczą. Ich zadaniem jest także dostosowanie swoich formularzy, komunikatów, e-maili czy też innych zapytań tak, aby były one jasne, zrozumiałe i czytelne dla przeciętnego odbiorcy. Istotą jest bowiem jakość przekazywanych w zapytaniu informacji, a nie ich liczba.

Unijny prawodawca wprowadził wiele nowych rozwiązań w celu wyznaczenia wzorów postępowania oraz interpretacji, które są nowością w stosunku do poprzednich regulacji. W związku z rozpoczęciem stosowania RODO wykształciły się nowe sposoby postępowania mające na celu realizację uprawnień osób, których dane są przetwarzane. Nie jest jednak lekceważony dotychczasowy dorobek literatury i orzecznictwa, a także doświadczenia związane ze stosowaniem przepisów zapewniających pełnię uprawnień osobie, której dane dotyczą. Coraz częstsza analiza skutków wynikających z naruszenia prawa do ochrony danych medycznych oraz kwestii wyrażenia i cofnięcia zgody na przetwarzanie danych być może spowoduje zwiększenie znaczenia tego prawa wśród społeczeństwa, a co za tym idzie zapewni pełną ochronę prywatności i autonomii informacyjnej pacjenta.

Słowa kluczowe: dane medyczne, dane genetyczne, dane biometryczne, prawa pacjenta, tajemnica lekarska

Informacje o Autorze: Mgr EDYTA MARCINIAK, doktorant w Katedrze Publicznego Prawa Gospodarczego, Instytut Prawa, Wydział Prawa, Prawa Kanonicznego i Administracji, Katolicki Uniwersytet Lubelski Jana Pawła II; Al. Racławickie 14, 20-950 Lublin, Polska; e-mail: solecka.edytka@gmail.com; https://orcid.org/0000-0002-0152-3802