

## **STRESZCZENIE**

### **„Ochrona medycznych danych osobowych”**

Tematem rozprawy są prawne zagadnienia związane z ochroną medycznych danych osobowych. Analizowana problematyka ma doniosłe znaczenie, bowiem dotyczy danych, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności i wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności (motyw 51 preambuły rozporządzenia 2016/679). Ponadto omawiane zagadnienie nabiera szczególnego znaczenia w dobie dynamicznego rozwoju technologii związanych z wymianą i gromadzeniem danych w ochronie zdrowia oraz olbrzymiego wzrostu wartości tych informacji i zagrożeń związanych z naruszeniem szczególnych kategorii danych.

Potrzeba dokonania analizy problematyki, stanowiącej przedmiot niniejszej rozprawy wynika w szczególności z faktu przyjęcia w dniu 27 kwietnia 2016 r. rozporządzenia 2016/679, które zaczęło obowiązywać od dnia 25 maja 2018 r. Zagadnienia, będące przedmiotem analiz w niniejszej rozprawie stanowią *novum* w polskim systemie prawnym, bowiem powstawaniu pracy towarzyszyła unijna reforma systemu ochrony danych osobowych i rozpoczęcie obowiązywania rozporządzenia 2016/679. Ponadto przyjęcie rozporządzenia 2016/679 wiązało się z koniecznością dokonania kompleksowej rewizji aktów prawnych w celu dostosowania obowiązujących przepisów prawa krajowego do nowych wymogów ochrony danych, wynikających z bezpośrednio obowiązującego rozporządzenia 2016/679

Podstawę analizy, przeprowadzonej w niniejszej pracy stanowią przede wszystkim rozporządzenie 2016/679, u.o.d.o. z 2018 r., ustawa z dnia 21 lutego 2019 r. zapewniająca stosowanie rozporządzenia 2016/679 oraz inne polskie akty prawne. W rozprawie uwzględnione zostały również wytyczne Grupy Roboczej art. 29 oraz przepisy projektu Kodeksu postępowania dla sektora ochrony zdrowia, wydanego zgodnie z art. 40 rozporządzenia 2016/679 dotyczącego podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających.

Rozprawa składa się ze wstępu, pięciu rozdziałów, podzielonych na podrozdziały oraz zakończenia. We wszystkich rozdziałach zawarte zostały uwagi ogólne, stanowiące wprowadzenie do analizowanej problematyki, a także uwagi końcowe, które stanowią podsumowanie rozważań, zawartych w poszczególnych rozdziałach oraz zawierają niejednokrotnie postulaty *de lege ferenda*. We wstępie określono przedmiot badań, cel i pytania badawcze oraz metody analizy naukowej.

Rozdział pierwszy ma charakter wprowadzający i obejmuje analizę podstawowych zagadnień z zakresu ochrony prawnej medycznych danych osobowych. W rozdziale pierwszym omówiona została również ochrona medycznych danych osobowych na gruncie przepisów prawa polskiego oraz rozporządzenia 2016/679.

Rozdział drugi rozprawy poświęcony został zagadnieniom związanym z przetwarzaniem medycznych danych osobowych. W pierwszej kolejności poczynione zostały uwagi wprowadzające dotyczące zasady bezpośredniego stosowania rozporządzeń. W dalszej kolejności został omówiony materialny i terytorialny zakres zastosowania rozporządzenia 2016/679. Następnie szczególna uwaga poświęcona została ogólnym zasadom przetwarzania danych osobowych oraz podstawom legalizującym przetwarzanie medycznych danych osobowych. Kolejną część rozdziału wypełniły analizy dotyczące przetwarzania medycznych danych osobowych z upoważnienia administratora lub podmiotu przetwarzającego oraz umowy powierzenia i podpowierzenia medycznych danych osobowych na gruncie przepisów rozporządzenia 2016/679.

W rozdziale trzecim scharakteryzowane zostały prawa osób, których medyczne dane osobowe dotyczą. W ramach niniejszego rozdziału dokonano podziału uprawnień podmiotu danych na cztery zasadnicze grupy: informacyjne, korekcyjne, zakazowe oraz pozostałe uprawnienia. W końcowej części rozdziału analizie poddano ograniczenia dotyczące korzystania z praw.

Czwarty rozdział rozprawy obejmuje analizę obowiązków administratorów i podmiotów przetwarzających związanych z przetwarzaniem medycznych danych osobowych. W tym samym rozdziale omówiony został również status i zadania inspektora ochrony danych.

W rozdziale piątym omówiona została odpowiedzialność za naruszenie prawa do ochrony medycznych danych osobowych. Punktem wyjścia do analiz było scharakteryzowane pojęcie naruszenia przepisów o ochronie danych osobowych. W dalszej części rozdziału przeanalizowane zostały szczegółowo podstawowe rodzaje odpowiedzialności związane z naruszeniem prawa do ochrony medycznych danych osobowych, tj. odpowiedzialność administracyjna, cywilna, karna oraz odpowiedzialność za naruszenie obowiązku zachowania tajemnicy osób zatrudnionych w służbie zdrowia.

Zakończenie pracy obejmuje wnioski końcowe, prezentujące uwagi *de lege lata* i postulaty o charakterze *de lege ferenda*.

Przeprowadzenie w niniejszej rozprawie analiz regulacji prawnych oraz poglądów prezentowanych w literaturze i orzecznictwie oraz sformułowanie na ich podstawie wniosków pozwoliło na wykazanie zasadności tezy, wyrażonej we Wstępie niniejszej

rozprawy, zgodnie, z którą rozporządzenie 2016/679 zapewnia wyższy poziom ochrony medycznych danych osobowych w stosunku do dotychczas obowiązujących regulacji z zakresu ochrony danych osobowych. W celu zapewnienia skutecznej ochrony medycznych danych osobowych niezbędne jest jednakże uwzględnienie specyfiki sektorowej w regulacjach dotyczących przetwarzania tej kategorii danych. W rozprawie wykazano, że wyższy poziom ochrony medycznych danych osobowych przewidziany na gruncie przepisów rozporządzenia 2016/679 przejawia się głównie we wzmocnieniu i doprecyzowaniu praw osób, których medyczne dane osobowe dotyczą, rozszerzeniu zakresu obowiązków podmiotów uczestniczących w przetwarzaniu medycznych danych osobowych, określeniu zasad odpowiedzialności za naruszenie ochrony danych osobowych oraz zapewnieniu równorzędnych kar za naruszenie tych przepisów w państwach członkowskich UE.

Zawarte w niniejszej rozprawie analizy polskich przepisów dotyczących ochrony medycznych danych osobowych ukazały jednakże sporo wątpliwości i problemów jakie wiążą się z zapewnieniem stosowania przepisów rozporządzenia 2016/679 w polskim porządku prawnym i ich praktyczną realizacją. Analizy i ustalenia, zawarte w niniejszej rozprawie pozwalają na dokonanie końcowej oceny poddanego analizie stanu prawnego oraz sformułowania postulatów *de lege ferenda*, zmierzających do ustalenia optymalnego kształtu regulacji prawnych dotyczących ochrony medycznych danych osobowych.

## ABSTRACT

### “Protection of medical personal data”

The subject of the dissertation is legal issues related to the protection of medical personal data. The analysed issue is of great importance as it concerns the data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms and thus merit specific protection as the context of their processing could cause significant risks to the fundamental rights and freedoms (recital 51 of the preamble to the Regulation 2016/679). In addition, the issue discussed takes on special significance in the age of dynamic development of technologies related to the exchange and collection of data in health care and the enormous increase in the value of this information and the threats associated with the violation of special categories of data.

The need to analyse the issues that are the subject of this dissertation results in particular from passing the Regulation 2016/679 on April 27<sup>th</sup> 2016, which came into force on May 25<sup>th</sup> 2018. The issues analysed in this dissertation are a novelty in the Polish legal system, as the writing of this dissertation was accompanied by the EU reform of the personal data protection system and the entry into force of the Regulation 2016/679. In addition, the adoption of the Regulation 2016/679 required a comprehensive revision of legal acts in order to adapt the applicable provisions of national law to the new data protection requirements resulting from the directly applicable Regulation 2016/679.

The basis of the analysis carried out in this dissertation is primarily the Regulation 2016/679, the Act on protection of personal data of 10<sup>th</sup> May 2018, the Act of 21<sup>st</sup> February 2019 ensuring the application of the Regulation 2016/679 and other Polish legal acts. The dissertation also took into account the guidelines of the Article 29 Working Party and the provisions of the draft Code of Conduct for the healthcare sector, issued in accordance with Art. 40 of the Regulation 2016/679 concerning entities performing medical activities and processors.

The dissertation consists of an introduction, five chapters, divided into subchapters and an ending. All chapters contain general remarks, constituting an introduction to the analysed issues, as well as final remarks, which constitute a summary of the considerations included in particular chapters and many times contain *de lege ferenda* postulates. The introduction specifies the subject of the research, the research goal and questions, the methods of the scientific analysis.

The first chapter has an introductory character and includes an analysis of basic issues in the field of legal protection of medical personal data. The first chapter also discusses the protection of medical personal data under the Polish law and Regulation 2016/679.

The second chapter of the dissertation is dedicated to the issues related to the processing of medical personal data. Firstly, the introductory remarks were made regarding the principle of direct application of regulations. Next, the material and territorial scope of application of the Regulation 2016/679 were discussed. Then, the special attention was given to the general principles of personal data processing and the legitimizing prerequisites of the processing of medical personal data. The next part of this chapter contains the analyses of processing of medical personal data under the authority of the administrator or the processor and contract for entrusting processing and sub-processing of medical personal data under the provisions of the Regulation 2016/679.

The third chapter characterizes the rights of medical personal data subjects. In this chapter, the data subject's rights were divided into four main groups: informative, corrective, prohibitive and other rights. In the final part of the chapter restrictions on the exercise of rights were analysed.

The fourth chapter of the dissertation includes the analysis of the obligations of controllers and processors related to the processing of medical personal data. This chapter also discusses the status and tasks of the Data Protection Officer.

In the fifth chapter the responsibility for violating the right to protection of medical personal data was discussed. The characterization of the definition of the violation of personal data protection regulations was the starting point for the further analysis in this chapter. In the further part of the chapter, the basic types of liability related to the violation of the right to the protection of medical personal data, i.e. administrative, civil and criminal liability as well as liability for violation of the obligation of confidentiality of persons employed in health care were analyzed in detail.

The ending of the dissertation includes final conclusions presenting *de lege lata* remarks and *de lege ferenda* postulates.

The analysis of legal regulations and views presented in the literature and case law conducted in this dissertation and the formulation of conclusions based thereon allowed to demonstrate the validity of the thesis, expressed in the Introduction of this dissertation, according to which the Regulation 2016/679 provides a higher level of protection of medical personal data compared to previously binding regulations on the protection of personal data. However, in order to ensure effective protection of medical personal data, it is necessary to take into account the sectorial specificities in the regulations regarding the processing

of this category of data. The dissertation also showed that the higher level of protection of medical personal data provided under the provisions of the Regulation 2016/679 manifests itself mainly in strengthening and clarifying the rights of the medical personal data subject, extending the scope of obligations of entities involved in the processing of medical personal data, determining the principles of liability for a violation of the protection of personal data and ensuring equivalent penalties for the violation of these provisions in EU Member States.

The analyses of Polish provisions regarding the protection of medical personal data presented in this dissertation also showed many doubts and problems associated with ensuring the application of the provisions of the Regulation 2016/679 in the Polish legal order and their practical implementation. The analyses and findings presented in this dissertation allow for the final assessment of the legal status which was considered and permit to formulate the *de lege ferenda* postulates aimed at determining the optimal shape of the legal regulations regarding the protection of medical personal data.