ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2021 (26)

# HEALTH DATA PROTECTION AS A MEASURE OF REALIZING AN INDIVIDUAL'S RIGHT TO PRIVACY

**Eglė ŠTAREIKĖ**
*Mykolas Romeris University*
*Maironio st. 27, LT 44211 Kaunas*
*E-mail egle.stareike@mruni.eu*
*ORCID ID: 0000-0001-7992-991X*

**Sigita KAUSTEKLYTĖ-TUNKEVIČIENĖ**
*Mykolas Romeris University*
*Maironio st. 27, Kaunas*
*E-mail sigitat@mruni.eu*
*ORCID ID: 0000-0002-7108-9482*

*DOI: 10.13165/PSPO-21-26-28*

***Abstract.*** *The quality protection of the fundamental right to privacy cannot be achieved without sufficient protection of personal data. The General Data Protection Regulation provides special rules for the* processing of health data *as a special category of personal data which is considered to be sensitive by its nature.*
*In this article we aim to investigate the legal regulation for the processing oh health data and to show the connection of this legal regulation with the individual's fundamental right to privacy. And vice versa – it's important to determine what impact the right to privacy has had on the law of personal data protection.*
*In order to achieve those goals, there will be discussed the origins of the right to privacy and it's enshrining into the international and local law. The article will analyze not only the legal regulation of health data protection, but also reveal the connection between individual's right to privacy and the personal data protection system.*

***Keywords:*** *right to privacy, health data processing and protection, regof lamentation of rigt to privacy and health data protection, GDPR.*

## Introduction

The rapid technological progress and use of information technology across numerous domains of society, the COVID-19 pandemic and processes of globalization have highlighted the importance of personal data protection and privacy. At the same tame it has led to re-examination of problems, arising from inappropriate processing of personal data, when the pursuit to protect individual's privacy is no longer sufficient.

The system of personal data protection was created in order to protect not only personal data, but also individual's right to privacy. Violation of the right to personal data protection also initiates a violation of right to privacy. The focus of personal data protection on the protection of privacy determines both the content of the legal provisions and their implementation in the field of personal data legal regulation. So the purpose of General Data Protection Regulation is to create a secure basis for fundamental human rights and freedoms and it does it through imposing a uniform data security law in all European Union which provides a higher level of personal data protection. The need to ensure privacy and personal data protection is set both in the legal systems of European Union and The Council of Europe, that are closely interrelated in ensuring the protection of fundamental human rights.

So the article defines personal data protection as the safeguarding of the privacy right of individuals in relation to the processing of personal data. The relation between personal data protection and right to privacy as well as the influence of this relation on the structure and the content of law on personal data protection is analyzed in the article too.

The first part of article is dedicated to analyze the relation between privacy and personal data protection, to discuss the legal regulation of those rights, to determine the values protected by those rights and to estimate the limitations of absoluteness. The next two parts of the article introduce the concept of health data as the special category of personal data and analyze the requirements for health data processing. There are also discussed health data processing breaches as an infringement of the right to privacy.

The relevance of this scientific article is related to identification of requirements for ensuring personal data processing and privacy and also the nature of violation.

The aim of this scientific article to analyze the legal regulation of health data processing and to identify the connection between this legal regulation and fundamental individual right to privacy.

The object of the scientific article is the processing of health data and responsibility for data processing breaches.

Methodology of the Research – method of comparative analysis, methods of logical – analytical and systematic analysis. The method of comparative analysis is applied to compare the content and legal regulation of the right to privacy with the right to personal data protection. The analysis of requirements for health data processing and the analysis of the nature of violations are based on a logical-analytical method. Methods of logical – analytical and systematic analysis are used to reveal the relationship between legal acts, legal doctrine and different legal norms, also to summarize the article, to disclose the main problems and to submit conclusions.

## The right to the protection to the protection of personal data as an expression oh the right to privacy

COVID-19 pandemic prompted states to take various restrictive measures of human rights to stop the spread of the virus and to protect human health and lives. The fight against the new coronavir has led to the collection of personal data and further highlighted issues related to privacy and the right to protection of personal data. The pandemic situation has resulted not only in the processing and collection of comprehensive data related only to health disorders, but also in other domains on subjects' behavior, relationships, personal lives, in an attempt to control the spread of the virus at all costs (Milaj, 2020). The threat not only to the protection of personal data but also to the right of privacy has again raised the question of the relationship between these two rights.

The right to privacy and the protection of personal data are guaranteed by the legal framework of both the European Union (hereinafter - the EU) and the Council of Europe (hereinafter - the CE), which ensures the protection of fundamental human rights. The right to privacy and the protection of personal data are closely interlinked, sometimes even overlapping rights, but they are not identical rights (although they defend similar values - human dignity, the right to autonomy, the secrecy of private life, etc.). There is an indisputable link between these two rights, but there is still no general consensus on the relationship between these two rights. However, an analysis of international and national documents suggests that data protection and privacy are not considered synonymous (Lukacs, 2020).

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms establishes the right of the individual to respect for his or her private and family life: (i) everyone has the right to respect for his private and family life, his home and his correspondence; (ii) there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society

in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Council of Europe, Rome, 1950).

Modernised convention for the protection of individuals with regard to automatic processing of personal data (Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 128th Session of the Committee of Ministers, Elsinore, Denmark 17-18 May 2018 (Council of Europe Convention 108+)), is the only legally binding multilateral agreement on personal data protection. The purpose of the Convention is to protect the right to privacy through automatic processing of personal data, to respect the rights and fundamental freedoms of everyone, regardless of their nationality or place of residence, to regulate international data transfers and, above all, to guarantee individuals' right to privacy.

According to the General Data Protection Regulation (hereinafter - GDPR), personal data are understood as (i) any information relating to an identified or identifiable natural person (data subject); (ii) an identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as name, personal identification number, location and internet identifier, or to one or more identifiers of that natural person; characteristics of a person's physical, physiological, genetic, mental, economic, cultural or social identity (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, hereinafter - GDPR).

The link between the use of the term is enshrined in most basic international and national legislation as the concept of the right to privacy, which often includes the protection of personal information. In addition, these concepts, although not identical, are closely interlinked: ensuring a person's right to privacy also guarantees the protection of his or her personal data, while guaranteeing the protection of personal data also protects the right to privacy. Information about persons that allows the identification of a person (for example, a person's name, surname, place of residence, health data, etc.) is understood as personal data (Malinauskaitė, 2015).

Meanwhile, Article 7 of the Charter of Fundamental Rights of the European Union (hereinafter EU Charter) (Charter of Fundamental Rights of the European Union (CFR), OL 7.6.2016, C 202/391) distinguishes between the right to private and family life, where everyone has the right to respect his or her private and family life, the inviolability of home and secrecy of the communications. And Article 8 of the EU Charter regulates the protection of personal data, giving everyone the right to the protection of their personal data, which must be properly processed and used only for specific purposes and only with the consent of the person concerned or on other lawful grounds (Article 8 of CFR).

The Article 29 Working Party (the European Data Protection Board, after implementation of GDPR) also stated in its opinion that on the one hand, it has to be considered that the concept of private and family life is a wide one, according to the European Court on Human Rights in the case Amann v Switzerland of 16.2.2000, §65 : "[...] the term “private life” must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of “private life”[...]".On the other hand, the rules on protection of personal data go beyond the protection of the broad concept of the right to respect for private and family life. The Article 29 Working Party also emphasized that the Charter of Fundamental Rights of the European Union distinguishes data protection as an autonomous right and separates it from the right to privacy

(Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136 (Article 29 Working Party)). Meanwhile, according to the ECHR, the protection of personal data is to be considered as an expression of the right to privacy.

According to some scholars, such as P. De Hert and S. Gutwirth (2006), three main elements justify the separation of the right to privacy from the right to data protection. First, data protection clearly protects values that are not at the heart of privacy, such as the requirements of fair, lawfulness, consent to the processing of personal data. Secondly, the separation and recognition of the right to data protection and the right to privacy respects the different constitutional traditions of Europe. Separating the two rights was also expressed in the framework of the consultative meetings for modernising Convention 108 (Council of Europe Convention 108+). Third, the need for personal data protection has increased particularly in response to new information technology challenges, so it was no longer appropriate to attribute these new challenges and problems to privacy breaches. Ensuring the right to privacy as a fundamental human right has become a challenging task in the age of advanced technology. According to M. Civilka (2001), such situation was caused by the fact that information related to the private life of individuals becomes a commodity of high commercial value. The ability to analyze information about customer and consumer habits and needs determines the competitive advantage of companies.

It can also be noted that the scope and wording of the right to privacy and the protection of personal data differ, as the possibilities of restriction, the supervisory authorities. It can be assumed that the right to data protection as a separate right has developed as one of the components of a person's private life. There are differences in the material scope of the right to privacy and the right to the protection of personal data, i.e. data protection covers only information that allows the identification of individual persons. The genesis of the right to data protection can also be distinguished: the first stage was the development of data protection rules, the second stage regulated the emergence of international personal data protection regimes and the third stage no longer emphasized the collection of personal data but the lawful transfer of data to third parties. The right to privacy requires that the state and its actors do not interfere in a person's private life, giving the person the right to self-expression, freedom of religion, freedom of association, and so on. Meanwhile, the right to data protection provides legitimate means of implementing control mechanisms whenever personal data are processed, so that the state or its institutions and private entities process personal data in accordance with the established rules. Thus, these two rights differ in the scope of their protection and the actors involved. However, although different, the two rights can be very closely linked and even overlap. In this case, one violation - can violate both rights at the same time (Milaj, 2020).

The right to the protection of personal data applies as soon as personal data are processed, regardless of what they are (name, surname, bank card number, e-mail address, etc.) or belong to special categories of data (personal racial data, or ethnic origin, political views, religious beliefs, trade union membership, genetic data, biometric data, health data, data on a person’s sexual orientation). Thus, in terms of the application of the law, it can be said that the protection of personal data is broader than the right to privacy. Illegal processing of personal data can reveal information about person's family and personal life, while violating a person's right to privacy. However, in order to prove a personal data breach, it is not necessary to prove that a person's right to privacy has been violated. Disclosure of specific data, such as personal health data on infection of HIV/AIDS, sexual life, can have a significant impact on a person's private life, professional activities, reduce opportunities for communication in society.

Another important aspect is that both the right to privacy and the protection of personal data are not absolute, so restrictions on these rights are possible in order to strike a balance while ensuring other human rights.

Convention no. 108+ of Council of Europe restricts the exercise of individuals' rights where they can be justified by overriding interests, such as the protection of state security, public security, the protection of the public financial interests, the prevention of crime, the protection of data subject or the rights and freedoms of other individuals (Council of Europe Convention 108+). The Charter of Fundamental Rights of the European Union establishes that personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or on some other legitimate basis laid down by law. Also, everyone has the right of access to data which has been collected concerning him or her, and the enforcement of such a right must be monitored by an independent authority.

Meanwhile, the right to privacy prohibits the conduct itself, which would violate such individual right, unless a restriction of the right to privacy is possible in order to protect other values. The exercise of the right to data protection does not restrict the right itself, but creates binding conditions that must be met in order to ensure proper data protection management.

Independent institutional oversight can be described as another moment of separation between the right to privacy and data protection. All violations related to the right to privacy are defended in the national courts of the states (for example, in Lithuania - in courts of general jurisdiction), and the European Court of Human Rights becomes the final instance in order to protect the right to privacy.

When analyzing personal data protection law, an independent supervisory authority operating in a specific state (for example, in Lithuania - State Data Protection Inspectorate) occupies a very important role when applying for and filing an initial complaint and in order to defend one's violated right.

Both EU and EC legislation oblige states to establish a national supervisory authority in accordance with their national law for the efficient processing and supervision of personal data. According to GDPR Article 51 each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union. Each supervisory authority shall perform these functions in its territory:

(i) monitor and enforce the application of this Regulation;

(ii) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(iii) advise other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights;

(iv) promote the awareness of controllers and processors of their obligations under this Regulation;

(v) handle complaints lodged by a data subject and other (Articles 51, 57 of GDPR)

Also in accordance with both GDPR and the Council of Europe Convention no. 108+ the following powers of the independent supervisory authority could be presented in a systematic way:

(i) notify the controller or processor of suspected personal data breaches;

(ii) warn the controller or processor that the intended processing operations may infringe the provisions of the data processing rules;

(iii) make reprimands to the controller or processor where the processing operations have infringed the provisions of the data processing rules;

(iv) impose an administrative fine;

(v) order the rectification or erasure of personal data, restrict their processing or prohibit the processing of personal data, etc. (Article 58of GDPR; Council of Europe Convention 108+).

In conclusion, the analysis of the legal regulation of the European Union and the Council of Europe leads to the conclusion that the right to privacy and the right to the protection of personal data are not identical rights, but are closely interrelated. The scope of the right to privacy and the protection of personal data, wording, possibilities of restriction, supervisory authorities differ. Advances in information technology, globalization processes, Covid-19 pandemic have highlighted in particular the importance of the right to data protection and the challenges that arise when the pursuit of an individual's right to privacy is no longer sufficient. Violation of one right may also lead to violation of another right. With this in mind, the next part of the scientific article will analyze the significance of health data protection through the prism of realizing a person's right to privacy. Further analysis reveals the circumstances or the unlawful processing and disclosure of personal health data violates the privacy of individuals. Also what are the requirements for the processing of personal data and what are the most common nature of breaches.

**The concept of health data and basis for processing**

Analysis of international and Lithuanian legal acts establishing the protection of privacy and examination of the concept of the right to privacy established in legal acts and legal doctrine show us, that information about natural person and adequate protection of this information is considered to be a part of privacy.

As personal data considered as one of elements of the privacy content, it is clear that collection, processing and the use of such data can have an impact on a person‘s privacy. Assurance of person‘s right to privacy also ensures the protection of personal data and vice versa – only the an adequate level of data protection will ensure the proper protection of private life. So one of the main goals and tasks of personal data protection law is to create and set standards of conduct which would be considered not violating the privacy.

The provisions governing personal data protection law can be divided into two groups (Petraitytė 2011):

- the first group include the rules, which set standards for the behaviour respecting an individual’s right to privacy when the personal data are being processed,
- the second group include the rules, which are setting out the measures, that a natural person may take to protect or defend his privacy as far as it is concerned to the processing of his personal data.

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 – GDPR - Regulation (EU) 2016/679) had made a fundamental reform of European Union data protection legislation. GDPR not only repealed Data Protection Directive 95/46/EC which was the basis of personal data processing rules in European Union. General Data Protection Regulation implemented the objective of the Member States of the European Union to reconcile fundamental human rights and freedoms, protection of privacy, technological progress and public security in the field of personal data protection.

General Data Protection Regulation recognizes data concerning health as a special category of data, which is considered to be sensitive by its nature. Processing is prohibited (Article 9(1) of GDPR) unless exceptions apply such as:

- the provision of the individual's explicit consent,
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent,
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing relates to personal data which are manifestly made public by the data subject;
- where processing is necessary for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes (State Data Protection Inspectorate, Recommendations on personal data protection aspects providing remotely healthcare services).

Requirements for the health data protection and confidentiality are implemented in Lithuanian national legislation. Article 2.23(2) of the Civil Code of the Republic of Lithuania states, that publication of data about person‘s health condition in violation of the procedure established by law, shall be considered as a violation of privacy. Article 8 of the Law on the Rights of Patients and Compensation of the Damage to their Health establishes not only the patient‘s right to the inviolability of his private life, but also determines the obligation to collect health data under the legal acts regulating of personal data and to ensure the protection of privacy when handling health data. However this law applies only to instutions, companies and other subjects providing health care services. In addition it should be mentioned, that none of the above specified nacional legistlation, neither EU Charter of Fundamental Rights or The European Convention on Human Rights provide a concept ot definition of health data.

Therefore General Data Protection Regulation, not only introduces a definition of health data, but also expands the concept of health data in two important aspects: content and the source of data (Januševičienė 2018).

The GDPR clarifies that health data covers not only the data concerning health, i.e. data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about that person's health status. The Regulation considers that health data may include information about the person collected in the course of the registration for, or the provision of, health care services, a number, symbol or particular assigned to a natural person to uniquely identify that person for health purposes, information derived from the testing or examination of a body part including from genetic data and biological samples or any information/conclusion on, for example, a disease, disease risk (i.e. data concerning the potential future health status of an individual), disability, medical history or the clinical treatment of the physiological or biomedical state of an individual, even independent of its source and the purpose of use (Clause 35 of Preambule of GDPR). Under the Regulation (EU) 2016/679 the purpose of the health data processing isnot necessarily related to health protection – for example the pharmacie‘s information about the antihypertensives, sold to their loyal clients, the results of assesments of child‘s maturity to study in primary education programs and etc.

Another important point is related to the source of health data. Health data are colected and processed not only in the way of providing healthcare, but also in life sciences industry, biological banks, insurance companies, pharmacies, at schools, in sports clubs, apps of smartwatches that records the activity and health status of data subject, in the State Social Insurance Fund Board under the Ministry of Social Security and Labour ant etc. So the GDPR does not establish an exhaustive list of sources from which the health, physical or medical condition of data subject can be predicted. Accordingly to this, the requirements and restrictions in GDPR for health data processing are mandatory not only for healthcare professionals, but for the whole subjects that process personal data corresponding to the content of health data.

**Requirements for health data protection and processing and responsibility for violation of GDPR rules**

The quantity and the type of health care information and so amount of health data have increased in recent years because of expanding numbers of available technologies for diagnosis and therapy and even the leisure. It means that the details now not only are bet must be recorded and thus become available for inspection by the others. Further, information on lifestyle (e.g., use of tobacco or alcohol), family history, and health status have become of greater interest and relevance as we learn more about the relationship of these factors to overall health and well-being. In addition, genetic data are becoming more readily available, not only for prenatal testing but also for assessing an individual's degree of risk for an inherited condition Health Data in the Information Age: Use, Disclosure, Privacy, 1994).

Data subjects (patients) generally understand that, with consent, information about their medical records or other kind of data concerning health will be shared widely within a health care center, hospital or within any other organization or institution. They also expect that data concerning health collected about them will be used only for the purpose of the initial collection and those data will not be shared with people or organizations not authorized to have such information and about which data subject must be informed.

Personal health data is by far the most sensitive category of personal data, which is increasingly becoming a target of cyberattacks and according to the Dutch Data Protection Authority's deputy chair Monique Verdier confirmation, „*the healthcare sector has consistently been in the top 3 sectors with the most data breaches in the past few years. And we're talking about a sector that stores a lot of highly sensitive personal data*" (Dutch DPA, 2021).

The Regulation obliges data controllers and processors to take as much responsibility as possible for the processing of personal data, and Article 5(2) of the Regulation is particularly important and significant in this context because of setting out the principle of accountability. The essence of this principle is that the data controller and data processor are not only responsible for compliance with data protection requirements, but must also be able to prove that the processing is carried out in accordance with the requirements of the GDPR.

Not only the establishment of the principle of accountability, but also the level of sanctions for data protection breaches is to be considered as another effective tool to promote the importance of the security of personal data. Article 83 of the Regulation lays down the criteria according to which the supervisory authority carries out the assessment and decides on the imposition/non-imposition of a fine and its amount. Depending on the nature of the infringement and other circumstances specified in the Regulation, the amount of the fine is differentiated and may reach up to 10 million EUR or up to 20 million EUR (or 2% or 4% from the total annual worldwide turnover of the previous financial year; whichever amount is higher)

(Article 83 of GDPR). Additionally it should be noted that the payment of the fine does not in any way protect neither data processor nor data controller from the obligation to compensate the individual pecuniary and non-pecuniary damage (Article 82(1) of GDPR).

Having examined the Regulation measures for ensuring data security, firstly it should be noted that each healthcare provider (and all other entities processing personal data relating to personal health) must comply with the general data processing principles set out in Article 5 of the Data Protection Regulation: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality and accountability.

In order to ensure the lawfulness of data processing, it is necessary to choose rightfully purpose of health data processing and to indicate the ground for data processing. The Regulation stipulates that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further processing of data for archival purposes of the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89 (1) shall not be considered incompatible with the original purposes (Article 5(1(b) of GDPR).

State Data Protection Inspectorate indicates, that in most cases and depending on the circumstances, health data are processed on one or more grounds, i.e. Article 6(1) (a) (patient consent), (b) (contractual obligation), (c) (legal obligation) or (d) (vital interests of the person) and one or more grounds of Article 9(2) (a) (patient consent), (c) (vital interests of the person) of the GDPR, (h) (provision of health care) and (i) (public interest in the field of public health).

Each health data processor and health data controller must select and establish appropriate technical and organizational measures to ensure compliance with the requirements of the GDPR. There are many different technical and organizational measures for ensuring personal data security, but in order to set or select an appropriate measure, it is recommended to evaluate the risks arising from data processing.

In accordance with Article 35(1) of the GDPR, where the type of processing (in particular when innovative technologies are used and taking into account the nature, scope, context and purposes of the processing) impose the risk for the rights and freedoms of natural persons, there must be the requirement to prepare the data protection impact assessment ('DPIA'). The DPIA is an important reporting measure as it helps data controllers not only to comply with the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. However, it is not necessary to carry out a DPIA for each processing operation. The list of data processing operations subject to data protection impact assessment was approved by Order No. 1T-35 (1.12.E) of 14 March 2019 of the Director of the State Data Protection Inspectorate.

Records of processing activities is another innovation introduced by the GDPR which is actual for handling of special categories of data and where the data processing operations must be described in details. These records can be considered as an internal data processing register of a company or organization, which describes all categories of processed data and processing operations.

Article 37(1) of the Regulation stipulates that the Data Protection Officer must be appointed in any case where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or;

- the core activities of the controller or the processor is the large-scale processing of specific categories of data or the large-scale processing of personal data on convictions and criminal offenses.

Thus, health care companies/institutions must appoint a DPO, while other institutions or bodies must assess the amount and content of the processed personal data.

The online website_https://www.enforcementtracker.com/ contains information about fines and penalties which data protection authorities within European Union have imposed under the GDPR.

Under decision of Data Protection Authority Rheinland-Pfalz made on the 3rd of December in 2019 the University hospital of the Johannes Gutenberg University in the German Region Rheinland-Pfalz had to pay a fine of 105,000 EUR for the insufficient technical and organizational measures to ensure information security (GDPR Enforcement tracker). The hospital had violated the Article 32 of GDPR multiple times during a mix-up of a patient at the admission of the patient. This resulted in incorrect invoicing and revealed structural technical and organizational deficits in the hospital's patient management.

For the same type of violation the Dutch Data Protection Authority impose a fine of 440,000 EUR on Dutch Haga hospital on the 18th of June 2019 (GDPR Enforcement tracker). The investigation of Dutch Data Protection Authority followed when it appeared that dozens of hospital staff had unnecessarily checked the medical records of a well-known Dutch person. The Dutch DPA concluded that the Haga Hospital had taken insufficient security measures with respect to authentication and the control of logging, which constitutes a violation of Article 32 of the GDPR.

The Spanish data protection authority on the 25th of February 2020, issued a resolution and fining HM Hospitales 1989, S.A. 48,000 EUR for violating Articles 5(1)(a) and 6(1)(a) of the General Data Protection Regulation – for insufficient legal basis for data processing (GDPR Enforcement tracker). In particular, the Resolution outlines that a complainant argued that at the moment of his admission in the hospital he had to fill a form including a checkbox indicating that, in case he did not tick the same, he agreed to the transfer of his data to third parties. In addition, the Resolution highlights that the form provided by HM was not compliant with the GDPR since consent was obtained through the inaction of the data subject.

On the 1st of December 2020 the Estonian DPA fined three online pharmacies 100,000,- EUR each for processing personal data without the consent of the data subjects - for insufficient legal basis for data processing (GDPR Enforcement tracker). The data in question are prescriptions for medicines of the data subjects. Third parties were able to view another person's current prescriptions in the e-pharmacy environment without their consent, based only on access to their personal identification code. The DPA highlighted that while it must be possible to purchase prescription drugs for other people, it is the responsibility of the company to ensure that the the prescription information is accessed with the consent of the prescription holder.

On the 17th of July 2018 Centro Hospitalar Barreiro Montijo has been fined 400,000 EUR by Portugueses Data Protectios Authority for three violations of GDPR. Investigation revealed that the hospital’s staff, psychologists, dietitians and other professionals had access to patient data through false profiles. The profile management system appeared deficient – the hospital had 985 registered doctor profiles while only having 296 doctors. Moreover, doctors had unrestricted access to all patient files, regardless of the doctor’s specialty (GDPR Enforcement tracker). So first was a violation of Article 5(1)(c), a minimization principle, by allowing indiscriminate access to an excessive number of users, and a violation of Article 83(5)(a) a violation of the processing basic principles. For those, the fine was 150,000 EUR. The second, a violation of integrity and confidentiality as a result of non-application of technical and

organizational measures to prevent unlawful access to personal data under Article 5(1)(f), and also of Article 83(5)(a), a violation of the processing basic principles. There, the fine was 150,000 euros. Finally, the hospital fined for 100,000 EUR under Article 32(1)(b), the incapacity to ensure the continued confidentiality, integrity, availability and resilience of treatment systems and services as well as the non-implementation of the technical and organizational measures to ensure a level of security adequate to the risk, including a process to regularly testing, assessing and evaluating the technical and organizational measures to ensure the security of the processing.

On the 26th of February 2021 Lithuanian Data protection Authority (DPA) imposed a fine of 12,000 EUR on the Lithuanian National Health Service (NVSC) for violation Articles 5, 13, 24, 32, 35, 58 (2) and 3,000 EUR on the company 'IT sprendimai sėkmei' violation Articles 5, 13, 24, 32, 35 of the General Data Protection Regulation The DPA had opened an investigation regarding a quarantine app introduced in Lithuania during the COVID-19 pandemic in spring 2020. The company 'IT sprendimai sėkmei' had developed the app, which was then used by the NVSC. In the course of the investigation, the DPA found that during the app's period of use, the data of a total of 677 individuals had been processed in varying degrees. The app was able to collect data such as the name, address and phone number of the data subjects. The DPA concluded that the controller had not taken sufficient technical and organizational measures to protect the data processing. Furthermore, a data protection impact assessment was not carried out, although this would have been necessary in particular because the app also processed special categories of personal data including health data. The DPA further stated that the controller had provided non-transparent and incorrect information in the app's privacy policy.

On the 11th of February 2021 The Dutch data protection authority, imposed a fine of 440,000 EUR on the Amsterdam hospital OLVG (GDPR Enforcement tracker). The Dutch DPA constituted a violation of Article 32 of the GDPR, as the hospital had taken insufficient measures between 2018 and 2020 to prevent access by unauthorized employees to medical records. This resulted, among others, in working students and other employees being able to access patient files without this being necessary for their work. Besides medical records, the patient files also contained, the social security numbers, addresses and telephone numbers of the data subjects.

After considering different decisions and the amounts of imposed fines for health data processing, it must be concluded, that data protection authorities are being particularly vigilant in the field of the handling of health data. It is not just because of the particular sensitivity of these data, but also for seeking to improve health data protection and to remind that requirements of GDPR for data processing are not just formality.

## Conclusions

The right to privacy and the protection of personal data are guaranteed by the legal framework of both the European Union and the Council of Europe, which ensures the protection of fundamental human rights. Both the right to privacy and the protection of personal data are not absolute, so restrictions on these rights are possible in order to strike a balance while ensuring other human rights.

The right to privacy and the protection of personal data are closely interlinked, sometimes even overlapping rights, but they are not identical rights (although they defend similar values - human dignity, the right to autonomy, the secrecy of private life, etc.). According to the ECHR, the protection of personal data is to be considered as an expression of the right to privacy.

Quality protection of privacy is not possible without the protection of personal data, including legal regulation of health data. General Data Protection Regulation redraws the limits of liability for compliance in data protection law and increases importance of personal data protection and privacy issues. The data controller must prove that the correct technical and organizational measures have been taken to protect the data and that the data processing complies with the GDPR. Because of the analysis and organization of processes related to the processing of personal data, substantial progress was made in health data protection having in mind the particular sensitivity of data. Information about the imposed fines confirms, that the requirements of GDPR for health data processing are not formal and declarative – they also contribute directly to the protection of privacy.

## References

1. Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. Available at https://ec.europa.eu/newsroom/article29/items/611236/en (Accessed: 15 April 2021).
2. Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (Accessed: 20 April 2021).
3. Civilka, M. Asmens duomenų apsaugos reguliavimas interneto kontekste, 2001. Available at http://media.search.lt/GetFile.php?OID=92932&FID=269994 (Accessed: 15 April 2021).
4. Charter of Fundamental Rights of the European Union, Council of Europe, Rome, 1950. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN (Accessed: 20 April 2021).
5. De Hert, P. J. A., & Gutwirth, S. Privacy, data protection and law enforcement: Opacity of the individual and transparency of power. In E. Claes, A. Duff, & S. Gutwirth (Eds.), *Privacy and the criminal law*, pp. 61-104, 2006.
6. Dutch DPA, OLVG hospital fined for inadequate protection of medical records. Available at https://autoriteitpersoonsgegevens.nl/en/news/olvg-hospital-fined-inadequate-protection-medical-records (Accessed: 5 April 2021).
7. European Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe, Rome, 1950. Available at https://www.echr.coe.int/documents/convention_eng.pdf (Accessed: 25 April 2021).
8. GDPR Enforcement tracker, viewed on the 15th of April 2021. Available at https://www.enforcementtracker.com/ETid-122 (Accessed: 15 April 2021).
9. GDPR Enforcement tracker. Available at https://www.enforcementtracker.com/ETid-63 (Accessed: 15 April 2021).
10. GDPR Enforcement tracker. Available at https://www.enforcementtracker.com/ETid-216 (Accessed: 15 April 2021).
11. GDPR Enforcement tracker. Available at https://www.enforcementtracker.com/ETid-518 (Accessed: 15 April 2021).

12. GDPR Enforcement tracker. Available at https://www.enforcementtracker.com/ETid-45 (Accessed: 15 April 2021).

13. GDPR Enforcement tracker. Available at https://www.enforcementtracker.com/ETid-555 (Accessed: 15 April 2021).

14. Health Data in the Information Age: Use, Disclosure, Privacy. Institute of Medicine (US) Committee on Regional Health Data Networks; Donaldson MS, Lohr KN, editors. Washington (DC): National Academies Press (US); 1994. Aivalable at https://www.ncbi.nlm.nih.gov/books/NBK236546/ (Accesssed: 14 April 2021).

15. Januševičienė J., Practical Issues of Health Data Processing According to General Data Protection Regulation, *Teisė*, 1070, pp. 111-128. Available at https://doi.org/10.15388/Teise.2018.107.11826 (Accessed: 7 April 2021).

16. Lazauskaitė, R; Tamulionienė, D. Asmens duomenų tvarkymo ypatumai nuotoliniu būdu teikiant paslaugas sveikatos priežiūros srityje. *Jurisprudencija*, [S.l.], v. 27, n. 2, p. 370–388, vas. 2021. Available at https://ojs.mruni.eu/ojs/jurisprudence/article/view/6364 (Accesssed: 9 April 2021).

17. Lukacs, A. Protection Of Employees' Right To Privacy And Right To Data Protection On Social Network Sites – With Special Regard To France And Hungary, Doctoral (PhD) dissertation, 2020. Available at https://core.ac.uk/download/pdf/333872675.pdf (Accessed: 29April 2021).

18. Malinauskaitė, I. Privatumas virtualiuose socialiniuose tinkluose kaip įstatymo saugoma vertybė. *Social Transformations in Contemporary Society*, 2015 (3) ISSN 2345-0126 (online). Available at http://stics.mruni.eu/wp-content/uploads/2015/07/STICS_2015_3_115-127.pdf (Accessed: 29 April 2021).

19. Mallappallil, M., Sabu, J., Gruessner, A., & Salifu, M. (2020). A review of big data and medical research. SAGE open medicine, 8, 2050312120934839. Available at https://doi.org/10.1177/2050312120934839 (Accessed: 15 April 2021).

20. Milaj, J. Safeguarding Privacy by Regulating the Processing of Personal Data – An EU Illusion?, *EJLT Euopean Journal of Law and Technology*, Vol. 11 No. 2, 2020. Available at https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaa025/6246144?searchresult=1 (Accessed: 14 April 2021).

21. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 128th Session of the Committee of Ministers, Elsinore, Denmark 17-18 May 2018. Available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf (Accessed: 15 April 2021).

22. Monteiro, A., First GDPR fine in Portugal issued against hospital for three violations. Available at https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/ (Accessed: 11 April 2021).

23. Petraitytė I., Asmens duomenų apsauga ir teisė į privatų gyvenimą, *Teisė*, 2011, t. 80, p. 163-174. Available at https://epublications.vu.lt/object/elaba:59632226/index.html (Accessed: 14 April 2021).

24. 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). Available at https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed: 23 May 2021).

25. Schuler, M., Health data and data privacy: challenges for data processors under the GDPR. Available at https://globaldatahub.taylorwessing.com/article/health-data-and-data-privacy-challenges-for-data-processors-under-the-gdpr (Accessed: 20 April 2021).
26. Skirta bauda dėl Bendrojo duomenų apsaugos reglamento pažeidimų programėlėje „Karantinas“. Available at https://vdai.lrv.lt/lt/naujienos/skirta-bauda-del-bendrojo-duomenu-apsaugos-reglamento-pazeidimu-programeleje-karantinas (Accessed: 20 April 2021).
27. Valstybinės duomenų apsaugos inspekcijos direktoriaus 2019 m. kovo 14 Įsakymas Nr. 1T-35 (1.12.E) „Dėl duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo“ (TAR, 2019-03-14, Nr. 4104) [The list of data processing operations covered by the requirements to data protection impact assessment under the Order No. 1T-35 (1.12.E) of Director of State Data Protection Inspectorate of 14 May 2019]. Availabale at https://www.e-tar.lt/portal/lt/legalAct/abb01940465511e9a221b04854b985af (Accesssed: 14 April 2021).
28. Valstybinės duomenų apsaugos inspekcijos rekomendacijos dėl asmens duomenų apsaugos aspektų teikiant sveikatos priežiūros paslaugas nuotoliniu būdu [State Data Protection Inspectorate, Recommendations on personal data protection aspects providing remotely healthcare services of 18 May 2020]. Available at https://vdai.lrv.lt/uploads/vdai/documents/files/Pacientu%20konsultavimas%20nuotoliniu%20budu%202020-05-19.pdf (Accessed: 9 April 2021).
29. Violations de données de santé: la CNIL sanctionne deux médecins. Available at: https://www.cnil.fr/en/node/120684 (Accessed: 21 April 2021).