

UDK: 342.738 : 061.1EU

341.645

Review paper

Ema Turnšek, PhD student

University of Miskolc, Hungary

E-mail: ema.turnsek@centraleuropeanacademy.hu

THE FOUNDATION OF THE RIGHT TO DATA PROTECTION IN EUROPE IN THE LIGHT OF HEALTH DATA

ABSTRACT

The paper consists of three major parts, the development and assessment of the fundamental legal acts in relation to the right to data protection, the analysis of the right to data protection in detail and the chosen cases in this field. Firstly, the article tries to elaborate on the development of data protection in EU and in Signatory States of the ECHR through the most significant legal acts and judgments that shaped the legal framework we have today. Secondly, the article delves into the comprehensive structure of the right to private and family life pursuant to Article 8 ECHR. It addresses the lengths of the article and the right to data protection as a sub-right of the right to private and family life pursuant to the Article 8 ECHR as well as it exposes its different aspects and its position according to other sub-rights under the same Article. Thirdly, the article introduces four different cases concerning the protection of health data in particular, exposing different issues and findings of the CJEU and the ECtHR. Finally, the article shall provide the reader with a wholesome picture on how the right to the protection of personal (health) data developed, how it is understood and what meaning does it have today, particularly in Europe.

Key words: data protection in EU, data protection in Europe, health data, the right to data protection, the right to privacy, ECtHR's data protection case law, CJEU's data protection case law.

1. INTRODUCTION

In general, it has become quite common for us to use various health and medical phone-apps daily and to enjoy services of technologically advanced healthcare systems. It may seem unimaginable; however, thirty years ago, medicine did not have as advanced and developed digital equipment, like operating robots or artificial wombs for example, as it has today. Indeed, medicine and healthcare have rapidly developed since the Covid-19 outburst, but these fields have not stopped progressing. Taking into account the development of artificial intelligence and informational-technology all together, now is the era of the biggest changing and

of major developments in medical, biomedical, informational-technological and healthcare sectors, which enhances the need for an adequate protection of personal (health) data.

In 2008, EU has already recognized the right to data protection as an autonomous, independent right by the Lisbon Treaty and its newly implemented Charter of Fundamental Rights of the European Union.¹ Nonetheless, this was not the first acquaintance between the EU Member States and the right to data protection. The CJEU has acknowledged human rights and particularly, the right to data protection in the context of Article 8 ECHR, prior to the adoption of the Charter. In 1970, the CJEU has set forth that the fundamental human rights are, admittedly, an integral part of the general principles of law, of which the protection is guaranteed by no other than the CJEU.² At the time, EU did not yet have the human rights enshrined in an act of fundamental nature such as the Charter, which is why this clarification of the CJEU was significant. The judgment further on provided that in the absence of the human rights inclusion in provisions of the EU's Founding Treaties, their protection could be extracted from the joint constitutional traditions of the EU Member States. Therefore, even at the time, when the right to data protection was not yet directly enshrined into the primary EU law, it has already been recognised and protected by the EU. In 1995, the EU adopted secondary legislation in this field – Directive 95/46/EC;³ the CJEU, however, in many cases still referred to the protection of data under the European Convention of Human Rights,⁴ which has also become an act of fundamental nature for the EU Member States.

One of the fundamental legal acts that implicitly includes and protects the right to data protection is ECHR and in particular, its Article 8, the right to private and family life. ECHR was created in post-war times, in 1950 and it was the first mechanism to take certain rights of the Universal Declaration of Human Rights⁵ and make them legally binding for the governments of signatory states.⁶

¹ Charter of Fundamental Rights of the European Union, OJ EU C 326, 26. 10. 2012., hereinafter: the Charter.

² Case 11-70 Internationale Handelsgesellschaft mbH v. Einfuhr- und Vorratsstelle für Getreide und Futtermittel from 17 December 1970.

³ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50 (hereinafter: Data Protection Directive).

⁴ European Convention on Human Rights (1950), hereinafter: ECHR.

⁵ UN General Assembly, Universal Declaration of Human Rights, 217 A (III), 10 December 1948, <https://www.refworld.org/legal/resolution/unga/1948/en/11563> [accessed 29 November 2024], hereinafter: UDHR.

⁶ The official website of the European Court of Human Rights, European Convention on Human Rights, <https://www.echr.coe.int/european-convention-on-human-rights>, 26 November, 2024.

Admittedly, the right means very little without the proper safeguards, which is now solved by having an independent international court – European Court of Human Rights (hereinafter: ECtHR) that is ensuring the proper implementation and respect of the rights set forth by the Convention.

Interestingly, the provisions of ECHR may be found as very broad or even quite indefinite. Consequently, we may find many different interpretations of each Article and that may put a question on their realization in practice. Such situation also creates critical (and even opposing) opinions among the scholars. In his article, Mahoney argues that such open language and structure of ECHR give the Court significant opportunities and a wide-open window for choosing various interpretations, making the Court “the law maker”.⁷ In this regard, De Blois exposed inconvenient situations, where “the most substantive provisions” of ECHR leave a lot of space for interpretations, and in this sense, become a basis of judicial discretion.⁸ Admittedly, such approach can significantly shake the legal certainty regarding the proceedings in front of the ECtHR and even puts a question on the legitimacy of its decisions.

The ECtHR has, in a way, become a source or a mechanism for finding compensations for victims that did not get any or were served with inadequate satisfaction within the domestic legal system. That being said, the ECHR's confrontation with technological changes is crucial especially when it comes to addressing the right to private and family life within the means of data protection. The technologies we know and use nowadays are incomparably more invasive than the machinery was 20, 30 or 50 years ago. Back then, the protection of private and family life served mainly as a protection from the interferences of the State, in the terms of surveillance and from interfering in their basic family affairs. There was no indication that people needed the protection of their IP address, their medical or health data in a health app or the protection of their biometric data. Now, the right to privacy extends to emails, other types of communication and other equipment⁹ that could in any way have an influence on individual's privacy or personal data, which was made possible only by the modern technology. The protection of privacy was pictured differently at the time when ECHR was written; however, the previously criticized broad wording of the ECHR enables itself to

⁷ Mahoney, P., *Marvellous Richness of Diversity or Invidious Cultural Relativism*, 19 Human Rights Law Journal, 1998. See also Mahoney, P., *Judicial Activism and Judicial Self-Restraint in the European Court of Human Rights: Two Sides of the Same Coin*, 11 Human Rights Law Journal, 1990, p. 57.

⁸ De Blois, M., *The Fundamental Freedom of the European Court of Human Rights* in: Lawson, R.; de Blois, M. (eds), *The Dynamics of the Protection of Human Rights in Europe*, 1994, p. 51.

⁹ Van Dijk, P.; van Hoof, F.; van Rijn, A.; Zwaak L. (eds.), *Theory and Practice of the European Convention on Human Rights*, Fifth edition, Intersentia, p. 732.

surpass the time changes and it allows the ECtHR to continuously make provisions relevant and applicable to this day.

All of the above is crucial, especially for the legal fields of data protection, medical law and for other areas of new technologies. To substantiate the latter, the article shall tackle the topic of the right to data protection in the light of the right to the respect of private and family life pursuant to the Article 8 ECHR. That shall be done by initially dividing and researching two aspects of the right with the use of analytical and case law research. Firstly, the paper shall examine the scope of this sub-right throughout the analysis of the Article 8 ECHR and through a comparison to some other rights incorporated in the same provision. Secondly, the article shall identify the position of the right in relation to the principal right to privacy, previous and presently valid legal acts and the well-established case law. These points will enable the reader to fully understand the purpose, meaning and lengths of the right to (health) data protection in Europe. Subsequently, the paper shall focus on a specific group of sensitive data, the health-related data, and demonstrate its importance, mainly on the basis of decisions of the two highest legal instances, the ECtHR and the CJEU. Besides presenting some of the reference cases, in this chapter, the paper shall also demonstrate some of the utmost important aspects of the protection of health-related data, the philosophy behind it, reasons and possible consequences of unlawful disclosures of such data. The whole text is mainly written with the use of analytical and case law research methods. All-together, the article at hand shall draw a full picture of the right to (health) data protection pursuant to the Article 8 ECHR and of the ECtHR's standing on this matter.

2. DATA PROTECTION IN THE LIGHT OF THE RIGHT TO THE RESPECT OF PRIVATE AND FAMILY LIFE UNDER ARTICLE 8 ECHR

In the digital era that we live in, personal data has become a new currency. The States as well as various supranational and international organizations have recognized that and stepped-up accordingly. When defining personal data or even more specifically – sensitive personal data, first acts and definitions that come to our minds are probably the ones from General Data Protection Regulation¹⁰ that is

¹⁰ 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) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88 (hereinafter: GDPR).

relevant for EU or American Privacy Protection Act,¹¹ relevant for the US. Admittedly, the two governing acts have so far more or less regulated the data protection framework on the secondary level – one in the EU and the other in the US territory. However, there are also acts that stipulate the fundamental basis for such acts and enshrine the right to data protection through international legal acts into the national or federal legal systems. In this regard, the article shall mainly focus on one of the primary sources of data protection in Europe, which is the ECHR and its Article 8.

2.1. The scope of the right to data protection under Article 8 ECHR

When focusing on the right to private and family life pursuant to Article 8 ECHR, it must be noted that it every person with the right to respect for their private life, family life, and also for their home and correspondence.¹² In the academic literature these four elements are often addressed as pillars, which are not strictly separated among themselves nor further on defined.¹³ Nonetheless these pillars in many cases align or cover each other. Meaning, every pillar focuses on a particular point of person's private sphere and even though they in principal differ from each other, its cores are so closely connected that dividing them may not be successful in many situations. For instance, what the sub-rights addressed within the means of the first pillar – the right to private life – have in common are more or less self-standing aspects of personhood and private sphere; for instance privacy, reputation, identity, sexual life, relationships with others and the outside world, physical and psychological integrity, reproductive rights etc.¹⁴ On the other hand, the right to correspondence could be understood as the pillar providing protection of the confidentiality of communication in different forms as well as in various situations.¹⁵ In the scope of the latter, the protection extends to letters, emails,

¹¹ American Privacy Rights Act of 2024. (2023-2024). H.R. 8818 -118th Congress (hereinafter: APRA).

¹² Article 8(1) ECHR.

¹³ Johansson, E., *Privacy and data protection in a digital age: In the context of health data protection in Europe*, Independent written essay within the field of Constitutional Law and Human Rights UMEA University, 2024, pp. 6-10.

¹⁴ Van Dijk, P.; van Hoof, F.; van Rijn, A.; Zwaak L. (eds.), *op.cit.*, p. 669. See also European Court of Human Rights (secretariat), *Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence*, 2022, pp. 21-23.

¹⁵ European Court of Human Rights, *Guide on Article 8 of the Convention – Right to respect for private and family life*, Council of Europe/ European Court of Human Rights, 2017, p. 66.

internet and data storage on computers as well as to different types of telephone conversations from either private place, business premises or even from prison.¹⁶ It may seem confusing when looking at the whole scope of Article 8 ECHR as it extends to so many different fields and rights (from privacy to the right to healthy environment, the right to abortion, data protection, sexual orientation etc.), and it may make us question how far in depth each of these rights will actually be protected. Interestingly, when it comes to the right to healthy environment, the ECtHR will assess the situation only to the extent of the influences or harm imposed to an individual from polluting the environment – the environmental damage as such will not be taken into account without a person being harmed in some way nor will it be taken into consideration as a core issue of a case. Therefore, when it comes to this particular sub-right, its boundaries and limitations are undeniable. Admittedly, it may not always be clear, whether a particular case will stand the complex assessment and obligatory requirements that are needed to be fulfilled to actually make a case in front of the ECtHR; but it is clear that if the obligatory conditions are met, there are some limits to the ECHR's focus and assessment in these matters. Surprisingly or not, that is not always the case.

In consideration, what are then the limits of the ECtHR's decisions and explanations in connection to the right to privacy and data protection in particular? The right to privacy was already considered as an important part of Article 8 ECHR at the time of its creation. The latter can be seen from its wording, but the specific right to data protection was back then not yet in the minds of the Convention's Founding Fathers and cannot be sensed directly from this Article. The right to data protection is therefore a relatively "newly incorporated right" in the means of Article 8 ECHR, just like the right to gender identity or the right to a healthy environment. Another interesting point of view was presented in a book, titled *Deep diving into data protection*, of which authors argued that data protection should not even be considered as a fundamental human right, rather as a tool at the service of our self-development.¹⁷ Further, the book explained that data protection should be merely understood as a result of the positive obligations of our modern democratic States to handle all the digital challenges in a way, to enable their citizens to fully enjoy their human rights in that particular State's territory.¹⁸ Contrary to the latter, the right to data protection has been well defined,

¹⁶ *Margareta and Roger Andersson v. Sweden* App. no. 12963/87 (ECtHR, 25 February 1992), para. 72; *Malone v. the United Kingdom* App. no. 8691/79 (ECtHR, 2 August 1984) para. 64; *Halford v. United Kingdom* App. no. 20605/92 (ECtHR, 25 June 1997) paras. 44-46; *Copland v. the United Kingdom* App. no. 62617/00 (ECtHR, 3 July 2007), para. 41.

¹⁷ Herveg, J. (Ed.), *Deep diving into data protection: 1979-2019 : celebrating 40 years of research on privacy and data protection at the CRIDS*, Larcier (Collection du CRIDS; No. 51), 2021, p. 468.

¹⁸ *Ibid.*

assessed and commented by the ECtHR in many aspects, in general as well as in detail, in the scope of numerous judgments decades ago.¹⁹ Even before the GDPR was adopted, ECtHR has already made some very important decisions, shaping the trajectory of the understanding of data protection as such.

Since sensitive groups of data need a superior protection *per se*, it is significant that the ECtHR covers the protection of such groups of data as well. For instance, the ECtHR has dealt with many cases relating to the specific protection of health-related data and took quite a restrictive stand in the events of invasive interferences into individual's private life through disclosures and other infringements of his/her medical data.²⁰ Notably, the protection of health data is not such a small field to cover. It extends to the processing of health data, which covers all the forms of transmission, exposure, disclosure, use in healthcare systems, hospitals as well as on the internet, at work, verbally in daily life, via apps or in any other form or place, not to mention health data's substantive side. There are many different definitions for it, however, the one that is presently the most relevant for the EU citizens is definitely the one from Article 4 GDPR.²¹ When defining "health data's substance", it should be also taken into account, which data is included in the term. Admittedly, the concept of health related data should be considered as broad as to extend to particular data because of their medical relevance, particular purpose and scale of data processing.²² As the Working party Article 29 stipulated back in 2015, it is not mandatory to establish illness in order to qualify particular data as health related data.²³ The ECtHR and CJEU tackled variety of cases answering such legal dilemmas, but the eye-opening revelation might be the fact that this is only one group of sensitive data and there are several more. This may confirm a subtle remark that the scope of one sub-right that falls under Article 8 ECHR differs from the other ones. However, such statement remains very relative as with the passing of time, social changes, global movements, technological developments and it's will, the ECtHR may eventually modify certain limits of the "old rights" and add certain "new rights" as it did since 1950 till today.

¹⁹ See for example *Gaskin v. the United Kingdom* App. no. 10454/83 (ECtHR, 7 July 1989); *Z v. Finland* App. no. 22009/93 (ECtHR, 25 February 1997); *Klass and others v. Germany* App. no. 5029/71 (ECtHR, 6 September 1978).

²⁰ See more about it in the next chapter.

²¹ First point of the Article 4 GDPR describes data concerning health as personal data that are in relation 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.

²² Verhenneman, G., *The Patient, Data Protection and Changing Healthcare Models: The Impact of e-Health on Informed Consent, Anonymisation and Purpose Limitation*, Intersentia, 2021, p. 104.

²³ Article 29 Working Party, Annex to the letter of 5 February 2015 to Paul Timmers on mHealth – health data in apps and devices.

2.2. The broader concept and the development of the right to data protection

Looking at it more broadly, the primary purpose of Article 8 ECHR is to protect an individual against third-party's arbitrary interferences with any of the four pillars mentioned, namely private and family life, home, and correspondence.²⁴ While the right may principally be of negative nature,²⁵ the member States are also given positive obligations to ensure that the rights enshrined in Article 8 ECHR are respected even as between private parties, which may involve the adoption of measures designed to secure respect for private life (even in the sphere of the relations of individuals between themselves).²⁶ Interestingly, for an individual to invoke the first paragraph of Article 8 ECHR, he must show that the alleged breach falls within the scope of at least one of the following values – private life, family life, home and correspondence.²⁷ Indeed, the individual's complaint may touch more than one of these, as for example a data breach may extend on private life and correspondence at the same time. However, it is the applicant's responsibility to substantiate at least one, whereas the Court may not always substantiate which pillar was breached in particular.²⁸ Admittedly, data protection can fall within the scope of at least one pillar if not more (theoretically it could touch any of the four). Accordingly, while the right to data protection is being recognised as one of the significant rights protected by the ECtHR and other international and domestic acts, the interpretation of data protection as *a tool at the service of our self-development* cannot hold up. What is more, the right to data protection may as well be seen as a very specific right or scope of rights, if proceeding from an assumption that the concept of data protection originates from the right to privacy.²⁹ The latter should be considered as an older and broader concept of the protection of person's private sphere in comparison to the right to data protection.³⁰ The occurrence and the need for data protection arose no later than in the 80's. In 1981, the Council of Europe recognized the need for a more detailed data protection framework and adopted the first international treaty to regulate the right of individuals to the

²⁴ European Court of Human Rights (secretariat), *Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence*, 1st edition, December 31, 2016, p. 8.

²⁵ Kroon and Others v. the Netherlands App. no. 18535/91 (ECtHR, 27 October 1994) para. 31.

²⁶ This principle was for the first time mentioned in Marckx v. Belgium App. no. 6833/74 (ECtHR, 13 June 1979). See also Evans v. the United Kingdom App. no. 6339/05 (ECtHR, 10 April 2007) para. 75.

²⁷ Bates, E. et al., *Law of the European Convention on Human Rights*, Fifth edition, Oxford University Press, 2023, p. 508.

²⁸ Ibid, 510.

²⁹ Turnšek E., The Right to Privacy and Data Protection in European Healthcare Systems With an Emphasis on the Relevant Case Law And European Legislation. *Medicine, Law & Society*, 17(1), 2024, pp. 96-97. <https://doi.org/10.18690/mls.17.1.89-108.2024>

³⁰ Ibid.

protection of their personal data. The treaty was named the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, better known as the Convention 108, which has been amended in 2018³¹. The latter still remains in place and is well-known as a Convention 108+, serving as a guide for many countries even outside the European territory – in Mexico, Tunisia etc. Interestingly, Council of Europe was not the only one making its first steps in this field – at the same time the Organization for Economic Cooperation and Development (hereinafter: OECD) provided guidelines³² with a similar content and later on EU followed as well. The later recognised the need for a specific regulatory of this field and in 1995, implemented the Data Protection Directive. While it may seem like a success, the later was not perceived as such. Intriguingly, when the Data Protection Directive was in force, CJEU – instead of using its secondary legislation (this particular directive) – chose to make its assessments regarding the respect of data protection on the basis of the Article 8 ECHR. In *Rundfunk*³³ case, which was one of the earliest cases regarding the Data Protection Directive before CJEU, the Court assessed the compatibility of a national auditing requirement with the Directive.³⁴ In its judgment, the CJEU assessed the position of the right to privacy in accordance with the Article 8 ECHR – it examined, if there was any interference with the right to privacy that would constitute an unlawful or justifiable breach of Article 8 ECHR. While CJEU put its entire focus to the Article 8 ECHR, it in a way disregarded the particular data protection rules, set out in the Data Protection Directive. As the Court rather replaced the right to privacy for data protection rules, *Lynskey* emphasized this could leave the public with an idea that the right to privacy substitutes the right to data protection and disturb the future relevance of data protection rules.³⁵ Furthermore, in cases

³¹ Convention 108 + Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, accessible here: [chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf](https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf), 3 January, 2025.

³² Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of*

Privacy and Transborder Flows of Personal Data, OECD Publishing, Paris 2002.

³³ Case C-139/01 *Österreichischer Rundfunk and Others* from 20 May 2003.

³⁴ *Lynskey, O., Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order*, *International and Comparative Law Quarterly*, 63(3), 2014, <https://doi.org/10.1017/s0020589314000244>, p. 575.

³⁵ *Ibid.*

Satamedia³⁶ and Promusicae³⁷, CJEU made some conclusions, stipulating that Data Protection Directive is the act that actually protects the right to privacy and that right to privacy is synonymous with data protection. Interestingly such approach did not change until the Bavarian Lager³⁸, where even the European Data Protection Board intervened.³⁹ To clarify, the key issue was that Data Protection Directive made literally no reference to the right to data protection as such and in result, CJEU could neither. That being said, the Data Protection Directive was not as successful after all.⁴⁰ Maybe the expectations would be lower and therefore accurate, if the directive's naming and whole purpose were not to enhance the protection of data, but the protection of privacy.

Notably, the right to privacy could be understood as a broader right that among other rights includes the protection of a right to data protection as a more specific and narrowly oriented right.⁴¹ In contrast, Lynskey is opposing to this point of view with credible argumentation, stating that the right to data protection includes a broader range of data and data related actions within its scope as well as guarantees more data-processing related rights to the individual (than the right to privacy).⁴² In my viewing, both statements are correct. Even though it may look like they are contradictory at first sight, it may be established that the right to privacy is a broader right in a general sense. The later undoubtedly includes more aspects of individual's private (and family) life, whereas the right to data protection is a more specific right, covering different aspects and narrower rights in the more specific field of data protection, which also covers aspects that the right to private and family life does not necessarily deal with. In some points they certainly cover each other, e.g. if someone breaks into your email account, it invades into your private sphere (the breach is made against the correspondence as one of four pillars protected by the Article 8 ECHR) and compromises the information that lays within that email account (it can lead to a disclosure,

³⁶ Case C-73/07 Tietosuoja-valtuutettu v. Satakunnan Markkinapörssi OY, Satamedia from 16 December 2008. In this preliminary ruling, the CJEU held that collecting, publishing, and commercially using individuals' income and asset data from public tax records constitutes processing of personal data under Directive 95/46/EC, and may fall under the journalistic exemption only if the sole purpose of it is public information – however, that is a subject of domestic courts' assessment.

³⁷ Case C-275/06 Promusicae from 29 January 2008. In the *Promusicae* case, the Court ruled that EU law does not oblige its Member States to require ISPs to disclose personal data in civil IP cases, emphasizing the need to balance copyright protection with privacy and proportionality principles.

³⁸ Case T-194/04 Bavarian Lager v. Commission from 8 November 2007.

³⁹ Lynskey, O., *op.cit.*, p. 575.

⁴⁰ *Ibid.*, p. 570.

⁴¹ Turnšek, E., *The right to privacy and data protection in European healthcare systems with an emphasis on relevant case law and European legislation*, *op.cit.*, pp. 89-108.

⁴² Lynskey, O., *op.cit.*, p. 582.

transmission of personal data in particular). Taking into account some other aspects – the two rights may as well be hardly connected or not connected at all – e.g. the right to privacy includes a prohibition of a third-person to invade into individual's home, whereas the right to data protection may enable an individual the right to be forgotten (a right to erase individual's data from a database). Although we are still discussing the same rights, in the last example we may hardly sense a connection.

Admittedly, it is interesting to see, how and to what extent ECtHR acknowledges a quite comprehensive right to data protection inside the scope of already established right to private and family life under Article 8 ECHR. Even if it may seem that the right to data protection brings to the table a wide scope of “new” narrower rights, I believe it is significant that such (groups of sub-) rights enjoy the adequate protection, including the protection of the highest instances like the ECtHR and CJEU. Nonetheless, such approach is raising the concerns regarding the legal certainty and legal safety in connection to Article 8 ECHR as well as it is exposing the question of the limitations and boundaries of the ECtHR and its discretion.

3. RIGHT TO DATA PROTECTION THROUGH THE ECtHR'S CASE LAW

To substantiate the previously written, let us examine the chosen cases of ECtHR and CJEU that deal with the protection of sensitive personal data, more particularly health data, and with that, also with the individual's privacy and one's right to the respect of private and family life. The cases will be explored (more or less) chronologically, each exposing the significant question, unresolved matter and/or the significant definition provided within the particular judgment that cannot be found directly in the legislation.

3.1. Defining the sope “health related data” in Lindqvist case

An important decision on the protection of personal data relating to health was adopted by the CJEU in the Lindqvist case⁴³, where the Court provided an indefinite scope of the so-called group of “personal health data”.

⁴³ Case C-101/01 Bodil Lindqvist from 6 November 2003.

The background of *Ms. Lindqvist* circles around her working as a catechist in the parish of Alseda in Sweden. Despite her very traditional profession, she took part in data processing course where one of her tasks was to create a website with an arbitrary theme. In 1998, she set up a website on her home computer, in which she included useful information for believers preparing for confirmation. Among other details, the website included quite a lot of personal information, even personal (health) data (such as descriptions, family relationships, telephone numbers) about 18 co-workers from the parish. For example, one of the colleagues was described as having an injured foot and as working part-time due to this health condition. At *Ms. Lindqvist's* initiative, the website was linked to the official website of their church. She did not ask nor inform her colleagues about her website or the use of personal information relating to them, which caused some resentment among some of the parties. Although she withdrew the page when she learned about the frustration among her colleagues, the public prosecutor had already noticed her wrongdoing on his radar and charged her for violating Swedish data protection law. The Swedish court referred the matter to the CJEU for a preliminary ruling and among other questions, asked if the information on the website, which included “the name of a person who has an injured foot and is on part-time work because of it” falls under the scope of data concerning health.

Essentially, the CJEU stressed that the term “health-related data” should be interpreted broadly. Accordingly, the term must cover information regarding all health aspects, considering physical as well as mental state of an individual's condition. The crucial point of this ruling lays in the recognition of mental and psychological illnesses, which are nowadays becoming more and more topical. It is easy to determine whether information is of health nature when someone catches a virus or breaks a leg. It is a completely different situation, when someone is diagnosed with a medical condition that does not outwardly show clear signs of illness. This CJEU's decision from 2003 remains relevant today, as it, in line with the provisions of currently valid act for this field – GDPR, endorses the amplitude on how (broadly) the health data should be interpreted.

Interestingly, the protection of health data has been recently quite drastically enhanced, not only because of the adoption of the GDPR, but also by a number of judgments, including cases C-667/21⁴⁴, Case C-446/21⁴⁵ (*Maximilian Schrems v.*

⁴⁴ Case C-667-21 *ZQ v Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts* from 21 December 2023. This case is significant, because the CJEU confirmed that non-material damages under Article 82 GDPR require causation, exclude fault in compensation assessment, and are limited to monetary redress.

⁴⁵ Case C-446/21 *Maximilian Schrems v Meta Platforms Ireland Limited, anciennement Facebook Ireland Limited* from 4 October 2024, paras. 70-74. In this particular case, the CJEU ruled that disclosing one's sexual orientation publicly doesn't permit broader data

Meta Platforms Ireland Limited) and C-252/21⁴⁶ (Meta Platforms Inc and Others v. Bundeskartellamt). The latter have in common a restrictive interpretation of the exemptions for the processing of personal health data pursuant to Article 9(2) GDPR. In principal, processing of sensitive groups of data (that are discovering one's religious beliefs, sexual orientation, health data etc.) is prohibited. In the scope of the listed preliminary rulings, the CJEU also touched the basic idea of the higher protection of processing of personal health data as processing of sensitive group of data, explaining its basis for such categorization is in their particular sensitivity.⁴⁷ Such level of sensitivity may lead to a serious interference with the fundamental rights to respect for private life and to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights in the event of a breach.⁴⁸ Therefore, despite the general prohibition of the processing of health- and other groups of sensitive data, the Article 9(2) GDPR provides a list of exceptions, particularly ten derogations, which are independent of each other and must therefore be assessed independently.⁴⁹ If in doubt, whether a particular data falls into one of those limited categories or not, the explanation must be restrictive. But if met, each stands as an adequate reason for processing of such data and is allowed.

The development is undeniable as well as expected. Back in the time of the conclusion of Lindqvist case, there was no GDPR and the technology was not as developed as it is today. However, in this reference case the CJEU made an important explanation that remains relevant.

3.2. The lengths of data concerning health in relation to the case I. v. Finland

In the following case, ECtHR explained that personal information in relation to a patient is, without a doubt, connected to his or her private life.⁵⁰ The latter is also a basis for the application of Article 8 ECHR and what is more, it is an implication

processing, and explained that targeted advertising must respect limits on data type and retention.

⁴⁶ Case C-252/21 Meta Platforms Inc and Others v Bundeskartellamt from 4 July 2023, paras. 66-70. In general, this case revolved around a question whether the competition authorities can rule on the compliance or non-compliance of the undertaking with the GDPR in the context of a decision on an abuse of a dominant position. Importantly, the CJEU ruled on all six legal basis to process data, further clarifying the interpretation of Article 6(1) GDPR.

⁴⁷ C-667-21 ZQ v Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts from 21 December 2023, para. 41.

⁴⁸ Ibid.

⁴⁹ Ibid, para. 47.

⁵⁰ I. v. Finland App. no. 20511/03 from 17. 7. 2008, para. 35.

regarding its scope, extending it to the specific (so-called sensitive) groups of data. In 2008, ECtHR ruled in a case *I v. Finland*, where the applicant's human rights were found to be breached in the light of Article 8 ECHR, reflecting throughout violations of many more rights than just one.

The case concerned a nurse, who was infected with HIV and employed at a public hospital. At the same hospital, she also attended an infectious diseases clinic in regard to her HIV infection. In connection to observations made by her colleagues, she suspected that they had illegally accessed and read her medical records and had become aware of her health state. The ECtHR stressed it is of crucial importance to respect the sense of privacy of a patient as well as to generally preserve his or her trust in the medical profession and health services.⁵¹ If the system fails to provide the latter, there is a serious danger that people would stop acquiring medical and health services and as a result, harm themselves or even worse, spread the disease onwards to a number of people. In the event of the latter, the health system may as well collapse. Since the applicant in this case was infected with HIV, the safeguarding of such sensitive data was significant – taking into account the potential issues that could arise from its disclosure.

What is more, stepping out of the box named “the Convention”, which directly defines a relatively small circle of rights the applicant's personal rights were violated on various levels. In addition to the violation of the respect for the right to dignity given by every modern democratic state, the colleagues' knowledge of her medical condition constituted violations of different rights, each putting its own pressure to the applicant's dignity. Colleagues' interference constituted a violation of the applicant's right to privacy, the right to data protection, even of the right to independently decide whether to inform third parties regarding her own health state and made an illegitimate disclosure of personal (health) data. In consequence, the employer did not renew her work contract and she was left without a job for nearly two years. Because of the wide circling rumours, she had to sell her home and move to a different place. Besides the economic loss and degrading social life, she also had to face a loss of reputation. Lastly, it was not only her reputation and private life that was affected, but also her son's.

While the national legislation provided an option to claim a compensation for damages, originating from an unlawful disclosure of personal data (even if only alleged) – that was not sufficient to protect the applicant's private life. As there was no concrete protection that could in practice prevent such disclosure from

⁵¹ Ibid, para. 38.

happening, the Court stressed that the State failed to provide the proper assurance for private life and declared a breach of Article 8 ECHR.⁵²

In my opinion, this case is an exemplary one for studying the protection of medical and health data. It shows how far-reaching and damaging may be the consequences that occur from the unlawful disclosure of health data. It also represents the vital role of healthcare workers, doctors and medical staff and the importance of their understanding of data protection. If only those colleagues knew how significant influence their rumours will have on applicant's life, the story would most probably turn differently. What is more, this case reached the ECtHR more than 15 years after this breach actually happened. That suggests the State failed to recognize the violations as well as it did not manage to provide applicant with the satisfaction she deserved. Importantly, a given right means very little without the proper safeguards, that is why the State has to be active in a way to provide the protection and the guarantees of such rights. Admittedly, each individual should know his rights and claim them or even fight for them whenever they are breached. However, in real life there are many situations, especially in healthcare, where data subject does not possess the proper knowledge or skills that would enable him to protect his rights (in hospitals and similar institutions, we commonly see many elderly people, kids, people with special needs). Because they are weaker parties and cannot protect themselves, the law should take care of that for them.

3.3. The relation between the right to data protection and the right to freedom of expression through the prism of Biriuk v. Lithuania case

In the following ECHR's case, the Court dealt with a different issue – it was weighing the limits and the boundaries between the right to protection of personal data and the right to freedom of expression.⁵³

A powerful Lithuanian newspaper shared an article on the front page of the issue about Gitana Biriuk, a lady from a small town in Lithuania and in a very inconvenient, even disturbing way mentioned she was infected with the disease. The newspaper wrote quite many statements (mentioning only a few, but there were more) like:

“Notoriously promiscuous thirty-year old Gitana Biriuk is already sick with this fatal disease ...”

“ G. Biriuk was infected with HIV by drug users who come to visit her ... ”

⁵² I. v. Finland App. no. 20511/03 from 17. 7. 2008, paras 47, 48, 49.

⁵³ Biriuk v. Lithuania, App. no. 23373/03 (ECtHR 25 February 2009).

"A man who had wandered in from somewhere lived in Gitana's house for a few years. After some time he went away and left "a present" [referencing to the infection of HIV] for the woman ..."

"... medics at the Pasvalys hospital confirmed that G. Biriuk is HIV-positive. The woman was taken to hospital with tuberculosis. Blood tests revealed that she was HIV-positive ..."

*"It is an unmarried mother of two children, G. Biriuk [...] the women in nearby villages are afraid that their husbands will bring the deadly virus home ..."*⁵⁴

Although the breach of personal data in this case is quite straight-forward, the other opinionated comments may be found as offensive, if not even more hurtful, as the disclosure of her infection. Although the sole wording does not suggest a promising society, it is, however, a newspaper's job to make the headlines as eye-catching as possible, even if in indecent way.

As it can be seen from one of the retrieved statement, the medical staff from local health facility, Pasvalys hospital, confirmed her infection. Gitana Biriuk sued the newspaper. With her first lawsuit, she was relatively successful, noting the Lithuanian court awarded her with a slightly smaller amount for damages. However, Ms Biriuk appealed and made a complaint, with which she demanded full and maximum legally admissible compensation. At second instance, the court reduced the amount of compensation she was already awarded with and intriguingly, this decision was later on confirmed by the Lithuanian Supreme Court. While the case did not end in her favours, Gitana Biriuk was left without a basis that could have given her the compensation for damages. Despite the fact that a violation of Article 8 ECHR had already been recognised by national courts, Gitana's case reached the ECtHR.

ECtHR did not follow the decision of the Lithuanian Supreme Court as it did not consider the local people's concerns for their safety as legitimate reasoning in any way, even less likely as justifying for the publications made about the applicant's state of health and her life style. The ECtHR took quite an opposite standing, affirming that the respect of the confidentiality of health data is crucial and publishing about the Biriuk's health status and her personal life is not justifiable. What is more, ECtHR stipulated that the respect of the confidentiality of health data is not significant only for the protection of a patient's privacy, but also for the preservation of that person's confidence in the medical profession and in the health services in general.⁵⁵ The Court referred to the explanation in the case of *Z v.*

⁵⁴ Ibid, para. 6.

⁵⁵ Ibid, para. 43.

Finland, stipulating such practice could lead to people rejecting any medical or health assistance, which could result in worsening their health status, endangering their lives or even, in the event of transmissible diseases, public health.⁵⁶

Additionally, this case stands out as well because of the alleged cooperation and actual confirmation of Gitana Biriuk's infection by the medical staff of Pasvalys hospital. The latter points to another breach, a breach of a professional secrecy, but the Court did not deal with that question in particular, because it falls outside of its jurisdiction. However, ECHR acknowledged it and assigned "particular significance" to that circumstance. Even though the Russian legislation at the time did include some norms regarding the protection of the confidentiality of health information of a person, the national courts still failed to apply proper safeguards. In regard to weighing the right to freedom of expression on one hand, and the right to private and family life on the other, the ECHR emphasized the need for a distinction between reporting facts, of which role is to contribute to a debate in a democratic society and "cheap" allegations about an individual's private life.⁵⁷ The latter is what happened in newspaper's article about Ms. Biriuk. The ECtHR even argued that such distinction is important in the events of known people. Meaning, in cases where an individual is known to the public, he or she may just like anyone else legitimately expect the protection of and respect for their private life.⁵⁸ At this point, it is necessary to be reminiscent on the ECHR's broad interpretation of the right to freedom of expression, where the ECHR set close to "no limitations–practice" in favour of the invasive media publishing. Whereas in the case of disclosures of medical or health related data, the ECHR took an opposite standing and signified the importance of keeping person's data private as its disclosure may have tremendous consequences, including stigmatization, damage on social, economic, private life and more. Even in cases of publicly known people the ECtHR took a stance and recognized that they are too entitled to have their health data protected despite their public exposure. In my understanding, that recognition itself emphasizes the distinction between the protection of personal and sensitive health data, and highlights the significant importance of the protection of health data in general.

What is more, ECHR substantiated its interpretation with the correct development of every human being's personality. Considering the latter, it is true that without the reassurance of the respect of the individual's private life, a human cannot truly and fully develop his or her personality, as he or she may get shrunk by fear, uncertainty, anxiety, etc. However, the protection of personal health data is not

⁵⁶ See also the case of *Z v. Finland* App. no. 22009/93 (ECtHR 25 February 1997) para. 95.

⁵⁷ *Biriuk v. Lithuania*, App. no. 23373/03 (ECtHR 25 February 2009) para. 38.

⁵⁸ *Ibid*, para. 38.

only significant in the terms of the development of one's personality, but also when it comes to other aspects of personal development or identity. It is especially important to maintain such data confidential when referring to person's HIV status or similarly sensitive conditions. In the light of such remarks, it must also be noted that the ECtHR addressed the general respect of confidentiality of health data as a vital principle for our society. The latter will be more thoroughly examined below, in the scope of a more recent case, *Y. G. v. Russia*, where the Court expressed its comment in a slightly clearer way.

3.4. The impacts of digital tools on the protection of personal (health) data in the light of *Y. G. v. Russia* case

In this case, the applicant was a patient, infected with HIV and hepatitis, being cured in Moscow Centre for the Prevention and Control of Aids. One day, his acquaintance told him he is familiar with his condition, about which he learned from a database bought at Savelovskiy Market in Moscow. Then, in order to contest the credibility of such information, the applicant (*Y. G.*) himself, bought a compact disc with this database from the exact same market. On the first page of this database, there was a name of the centre, particularly the one's that he was registered with – Moscow Centre for the Prevention and Control of Aids. The collection consisted of personal data from more than 400,000 individuals infected with HIV, AIDS and hepatitis from Moscow area and elsewhere. The applicant found information related to him and among his personal data, there was also a statement between the notes, saying the applicant was “a hooligan, thief and drug addict, suffering from AIDS and hepatitis”.⁵⁹

Once more, the ECtHR very specifically stipulated that the protection of personal data and medical data in particular, is of fundamental importance for individual's enjoyment of his or her right(s) guaranteed by Article 8 ECHR.⁶⁰ Furthermore, the ECtHR emphasized the previously exposed key point on maintaining the confidence in healthcare system and medical profession. But most importantly, the Court identified that respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the ECHR.⁶¹ Notably, the disclosure of such sensitive health data to the public may have an extremely negative impact on the individual's respect for private and family life, on his or her social and professional standing as well as to his viewing in the society - it may cause stigmatisation and possibly even an exclusion from the society. While

⁵⁹ *Y.G. v. Russia* App. no. 8647/12 (ECtHR, 30 November 2022) para. 10.

⁶⁰ *Ibid.*, para. 44.

⁶¹ *Ibid.*

it has already been established that the protection of personal (health) data is undoubtedly included in the scope of the right to respect for private and family life in the sense of Article 8 ECHR, here the Court essentially implied it represents a crucial part of it. Because of its significant importance for an individual as well as for the general public, the national law is pressured to guarantee proper safeguards that will enable the respect of the right to data protection and also prevent such disclosures of individual's personal health data in line with the means of Article 8 ECHR.

The latter is especially relevant nowadays. Indeed, the technologies and information-technology systems are increasingly developing and therefore new developments and innovations are on the horizon every other year. However, law on the other hand develops slowly and the legislation in the making that lays in the cross-roads of medical law, digital health and data protection needs changing. The need of the latter is crucial, because of the continuous transferring of the tasks and parts of healthcare administration and medical services online, where the personal data is undergoing automatic processing. Some EU Member States have already taken the steps to regulate digital health and new health databases, which have already been predicted in 2004 under the EU's eHealth Action Plan.⁶² However, in the case of *Y. G. v. Russia*, the national bodies failed to do so, the safeguards were not set appropriately and as a result, the applicant faced damages that he should not. The ECtHR argued that Russia did not comply with its positive obligations and was therefore found to be in the breach of Article 8 ECHR.

Admittedly, back in the times when so advanced digital equipment has not yet existed, it was not possible to run the automatic processing – therefore, the same safeguards that are a must today were not even needed. Thus, in this rapidly developing era, it is a must for the Signatory States to take active steps to remain informed about the progress and innovations in order to ensure an adequate legal framework. For a particular State that can be achieved in different ways. When looking at it most generally, to keep its legislation lawful and up to date, the State should accordingly change its legislation and measures to ensure the effective safeguards that shall prevent its citizens from having their fundamental human rights breached.

In conclusion, pursuant to this case the ECtHR's decision is not only relevant because of setting the respect for the confidentiality of health data as a vital principle of all Signatory States, but also because it emphasized the general need

⁶² Turnšek, E., *Varstvo osebnih podatkov kot temeljna človekova in pacientova pravica*. Master's thesis. Maribor, Digital Library of the University of Maribor, 2024, p. 13. Retrieved from: <https://dk.um.si/IzpisGradiva.php?lang=slv&id=89430> (12. 4. 2025).

for the Signatories to provide the appropriate safeguards and measures as States' positive obligation. It is not the first time that the ECtHR provided such obligation for a State, but it is a very recent case, which makes it even more relevant and applicable for other Signatory States in this time.

4. CONCLUSION

Admittedly, the right to data protection is a more modern or a new right in comparison to the right to privacy, nevertheless it is seriously and wholesomely taken into account internationally, for example in Europe especially by the ECtHR and CJEU, despite not being directly included in the wording of the Article 8 ECHR. Its significant importance was soon recognised by the EU, which can be seen from the adoption of the legal acts in the field of data protection as well as from the enshrinement of the specific right to data protection in the Charter.

It can be concluded that the right to data protection has conquering rights on different levels. When it comes to more distant rights within the means of Article 8 ECHR, like in the example of comparing the right to a healthy environment with the right to data protection, the differentiation between the two is more obvious and the lengths of each right may be seen more clearly. In the comparison, we found that the right to data protection was so far examined in the scope of higher number of cases, from more aspects and by now, more questions in its regard were addressed. The comparison made was very broad. On the other hand, when we compare the right to data protection with the right to privacy, the distinctions between them are not seen as easily without understanding the full meaning and purpose of each and diving into details. The right to privacy includes different aspects of person's private sphere, it covers more of the broader rights, such as the right to home, correspondence, sexual life, identity, family life, gender orientation, and many more. While the right to data protection consists a wide pool of rights too, these right are narrower and extend to less fields than those sub-rights under the right to privacy. That does not mean the right to privacy is not broad – it actually covers many important questions and very topical issues.

In fact, there are some groups of data that should be and are more specifically protected from the other, because of their sensitivity. The sensitivity of health-related data in particular may lead to serious violations of basic human rights. That is why we categorize health data as one of the sensitive groups of data. Furthermore, the article tried to focus on the specific protection of only one of the sensitive groups of data, namely health-related data, and expose some important imputes of the CJEU and mostly, of the ECtHR. The CJEU established that health-related data concern not only physical, but also mental aspects of an individual.

Meaning, when someone has a mental health disease or a condition, that data shall not be excluded from the special protection in the scope of sensitive (health) data. What is more, the ECtHR established a very high level of the protection of health data, which every person is entitled to. However, that is not absolute. In comparison, when balancing the right to data protection in the scope of Article 8 ECHR and the right to freedom of expression under Article 10 ECHR, the full enjoyment of the right to data protection is not definitely or completely granted. Meaning, the right to data protection can be limited by the rights of the Article 10 ECHR and, therefore, in cases of some publicly recognised persons, such as politicians, actors, the royal family the protection of personal data will not be the prevailing right. It is generally understood that by having an established public recognition, these “famous” people consciously or purposely decide they are going to be spoken about by various media providers and by different platforms. That is why their enjoyment of the right to data protection is considered differently. However, when it comes to the right to the protection of health or medical data, even such people are entitled to it. The reasoning for such a strong protection of this type of data lies in the overarching importance of the confidentiality of health. The latter is crucial for maintaining the trust in medical profession and health services and to maintain the higher level of public health as well as to protect the most intimate parts of individual’s private sphere and allow him to enjoy the privacy of the data that may stir up most if not all parts of his life and relationships. In this regard, the ECtHR addressed health-related data as being a vital principle in the legal systems of all the Signatory States. That is why the national law is pressured to guarantee proper safeguards that will enable the respect of the right to data protection in practice and prevent such disclosures of individual’s personal health data in line with the means of Article 8 ECHR. With that, States are given not only negative obligations (to not interfere with persons’ private and family life), but also positive obligation to – actively and in the most efficient way – protect the rights of the Article 8 ECHR.

REFERENCES

BOOKS AND ARTICLES

1. Bates, E. et al., *Law of the European Convention on Human Rights*, Fifth edition, Oxford University Press, 2023, pp. 508-510.
2. De Blois, M., *The Fundamental Freedom of the European Court of Human Rights* in: Lawson, R.; de Blois, M. (eds), *The Dynamics of the Protection of Human Rights in Europe*, 1994, p. 51.

3. European Court of Human Rights, *Guide on Article 8 of the Convention – Right to respect for private and family life*, 2017, p. 66.
4. European Court of Human Rights (secretariat), *Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence*, 1st edition, December 31, 2016, p. 8.
5. European Court of Human Rights (secretariat), *Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence*, 2022, pp. 21-23.
6. Herveg, J. (Ed.), *Deep diving into data protection: 1979-2019 : celebrating 40 years of research on privacy and data protection at the CRIDS*, Larcier (Collection du CRIDS; No. 51), 2021, p. 468.
7. Johansson, E., *Privacy and data protection in a digital age: In the context of health data protection in Europe*, Independent written essay within the field of Constitutional Law and Human Rights, UMEA University, 2024, pp. 9-10.
8. Lynskey, O., *Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order*, International and Comparative Law Quarterly, 63(3), 2014, <https://doi.org/10.1017/s0020589314000244>, pp. 570, 570, 582.
9. Mahoney, P., *Marvellous Richness of Diversity or Invidious Cultural Relativism*, 19 Human Rights Law Journal, 1998, p. 2.
10. Mahoney, P., *Judicial Activism and Judicial Self-Restraint in the European Court of Human Rights: Two Sides of the Same Coin*, 11 Human Rights Law Journal, 1990, p.57.
11. Organization for Economic Cooperation and Development, OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Publishing, Paris 2002.
12. Turnšek, E., *Varstvo osebnih podatkov kot temeljna človekova in pacientova pravica*, Master's thesis, Digital Library of the University of Maribor, 2024, p. 13. Retrieved from: <https://dk.um.si/IzpisGradiva.php?lang=slv&id=89430> (12. 4. 2025).
13. Turnšek, E., *The right to privacy and data protection in European healthcare systems with an emphasis on relevant case law and European legislation*, Medicine, law and society, 17(1), 2024, pp. 89-108.
14. Van Dijk, P.; van Hoof, F.; van Rijn, A.; Zwaak L. (eds.), *Theory and Practice of the European Convention on Human Rights*, Fifth edition, Intersentia, pp. 669, 732.
15. Verhenneman, G., *The Patient, Data Protection and Changing Healthcare Models: The Impact of e-Health on Informed Consent, Anonymisation and Purpose Limitation*, Intersentia, 2021, p. 104.

LEGAL ACTS

1. American Privacy Rights Act of 2024. (2023-2024). H.R. 8818 -118th Congress.
2. Article 29 Working Party, Annex to the letter of 5 February 2015 to Paul Timmers on mHealth – health data in apps and devices.
3. European Convention on Human Rights (1950).
4. Charter of Fundamental Rights of the European Union, OJ EU C 326, 26. 10. 2012.
5. Convention 108 + Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, accessible here: chrome-extension://efaidnbmninnbpcajpcglclefindmkaj/https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf, 3 January, 2025.
6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.
7. 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) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88.
8. UN General Assembly, Universal Declaration of Human Rights, 217 A (III), 10 December 1948, <https://www.refworld.org/legal/resolution/unga/1948/en/11563> [accessed 29 November 2024].
9. Privacy and Transborder Flows of Personal Data, OECD Publishing, Paris 2002.

COURT DECISIONS

1. Biriuk v. Lithuania, App. no. 23373/03 (ECtHR 25 February 2009).
2. Case C-101/01 Bodil Lindqvist from 6 November 2003.
3. Case 11-70 Internationale Handelsgesellschaft mbH v. Einfuhr- und Vorratsstelle für Getreide und Futtermittel from 17 December 1970.
4. Case C-446/21 Maximilian Schrems v Meta Platforms Ireland Limited, anciennement Facebook Ireland Limited from 4 October 2024.
5. Case C-667-21 ZQ v Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts from 21 December 2023.

6. Case C-252/21 Meta Platforms Inc and Others v Bundeskartellamt from 4 July 2023.
7. Case C-139/01 Österreichischer Rundfunk and Others from 20 May 2003.
8. Case C-275/06 Promusicae from 29 January 2008.
9. Case C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi OY, Satamedia from 16 December 2008.
10. Case T-194/04 Bavarian Lager v. Commission from 8 November 2007.
11. Copland v. the United Kingdom App. no. 62617/00 (ECtHR, 3 July 2007).
12. Evans v. the United Kingdom App. no. 6339/05 (ECtHR, 10 April 2007).
13. Gaskin v. the United Kingdom App. no. 10454/83 (ECtHR, 7 July 1989).
14. Halford v. United Kingdom App. no. 20605/92 (ECtHR, 25 June 1997).
15. Klass and others v. Germany App. no. 5029/71 (ECtHR, 6 September 1978).
16. Kroon and Others v. the Netherlands App. no. 18535/91 (ECtHR, 27 October 1994).
17. Malone v. the United Kingdom App. no. 8691/79 (ECtHR, 2 August 1984).
18. Marckx v. Belgium App. no. 6833/74 (ECtHR, 13 June 1979).
19. Margareta and Roger Andersson v. Sweden App. no. 12963/87 (ECtHR, 25 February 1992).
20. Y.G. v. Russia App. no. 8647/12 (ECtHR, 30 November 2022).
21. Z v. Finland App. no. 22009/93 (ECtHR 25 February 1997).

NETWORK RESOURCES

1. The official website of the European Court of Human Rights, European Convention on Human Rights, <https://www.echr.coe.int/european-convention-on-human-rights>, 26 November, 2024.