UDC: 342.738:613]:340.13(73)
342.738:613]:341.24(4-672ЕУ)
DOI: https://doi.org/10.46763/BSSR242424179t

THE PROTECTION OF SENSITIVE PERSONAL DATA AND PRIVACY IN THE US AND EU WITH A FOCUS ON HEALTH DATA CIRCULATING THROUGH HEALTH APPS

Ema TURNŠEK

PhD candidate at the Ferenc Deák Doctoral School of Faculty of Law of the University of Miskolc
E-mail: ema@turnsek.com

Suzana KRALJIĆ

Full Professor at the Faculty of Law, University of Maribor
E-mail: suzana.kraljic@um.si

Abstract

In today's modern world, we have more than one global actor leading the economy and rapid technological development. The article focuses specifically on the right to sensitive data protection, or more broadly the right to privacy, in American and in EU legal system. This paper shows distinctions between the two and systematically demonstrates the protection of personal data in EU through years. Exploring these distinctions and different interpretations of the right to data protection is significant, because of the potential impacts on the consumer in particular, possibly resulting in being granted different rights when acquiring services in the EU or America.

We will also analyse the fundamental legal acts, which are the cornerstones of data privacy. As its main focus, the article will also examine the provisions concerning sensitive personal data, in particular health data. Furthermore, the article will study some specific concerns in connection to the American smart phone, smartwatch and computer health apps that are not fully compliant with basic EU legal principles, human rights or the General Data Protection Regulation. While the technology is so advanced and users may access these apps from anywhere across the world, such apps, and their privacy policies or other typical contracts, should comply with the relevant legislation, valid in the state of user's nationality or remaining. The paper examines and substantiates the latter through two recent cases. In one, data breaches were punished by imposing a relatively high fine, and in the other case

example, no punitive action was yet taken. That being said, the article argues the insufficient data protection framework that does not necessarily provide a consumer with appropriate safeguards, which is especially relevant in cases of transmission of personal health data.

Keywords: *data protection, privacy, sensitive Data, EU vs. US Legal Systems, health Data*

1. Introduction

In order to tackle the loopholes of data protection adequately, we must first understand the ideology of this legal branch and articulate the meaning of its basic institutes and terms. Admittedly, almost every person possesses a smart phone, a computer and maybe even a smartwatch. These technologically advanced devices are fully equipped with various apps, geolocation systems, an extensive amount of personal data and more. Many apps have been developed for health purposes, such as measuring quality of sleep, steps taken per day, monitoring of menstruation cycle, and consultations for mental health issues, to name only a few. While it is not usual for app providers to claim so, some apps may even trick users into believing those can serve as the source of help for mental health issues or sort of medical advisory. In most cases, these apps are free of charge and available to everyone.

Since users rarely read the typical contracts when registering in the app, it may seem as completely irrelevant if these are provided or not. However, users always need to agree with privacy policies and terms of conditions of such apps, even if that is only a formality, because in reality that usually means users agree without reading these documents. Here is the point where privacy and data protection concerns arise. Does a random individual know what value their personal data has and for what purpose these data may be processed? Are the privacy policies or the terms of use contracts written in a way as to protect the individual as a consumer and user of the app or will they and their data be left in the virtual world without adequate protection and safeguards? These are the significant issues, which shall be broadly examined and thoroughly elaborated through the article.

First, the article will explain the broader right of privacy and data protection in the American and EU legal systems and then compare them for a better understanding of the topic. Second, because of major distinctions between the two, American and EU perception of the right to privacy, the article will delve into the fundamental legal acts established in the EU and provide not only an overview of the data protection development in Europe but also define the meaning of personal data. Third, and most importantly, the article focuses on sensitive personal health data and examines the applicability of actual privacy protection in apps connected to health. The two chosen cases substantiate the

theory and draw a better picture of the topic and problems in practice. Admittedly, even if differently strict, both the EU and US have regulated this field. The problem arises in cases where American providers offer services of such apps to people who remain on the territory of EU and do not adjust their privacy policies to the stricter GDPR.

2. Right to data protection

The concept of privacy has been altered to a significant extent due to the rapid development of internet and various social platforms (Mastracci and Salemme, 2024). Personal data and its sharing have become a modern currency in exchange for modern services, whether that means sharing one's personal data to acquire a particular medical service, or only to be able to use a certain phone app or even internet connection. Although we live in a globalised world with well-functioning international markets, insurance systems and worldwide business models, we can still find some significant differences between the principal institutes of two major legal systems, comparing specifically the right to data protection and privacy in Anglo-American and Continental legal systems.

Admittedly, EU Member States (hereinafter: Member States) have harmonized and, in some aspects, even unified their domestic laws not only to promote the goals of an internal market but also to achieve better cooperation among them. For example, activities such as transmitting personal data or acquiring different health services in the EU (by the citizens of the EU) should be a user-friendly experience. In comparison to the EU system, the Anglo-American legal system, while sharing similar fundamental rights, is based on different core values and beliefs, and laws with different meanings. In other words, some very basic concepts have developed in the Anglo-American legal system in ways very different from those in the EU. A simple example of this distinction can be found in the understanding of the right to data protection and the right to privacy.

a. The American concept of data protection

The American concept of the right to privacy pursues the goal of "being left alone" (Warren and Brandeis, 1890). Intriguingly, personal data protection laws in the US are not consistent with this overarching norm, as they are weak and do not provide strong legal protection for a US citizen's protection of their private data, choices and activities (James, 2014, p. 257). In general, the public interest in protecting the right to personal data in the US is weaker. This is seen through less restrictive regulations in terms of privacy and protection of personal data (Baumer, Earp and Poindexter, 2004). The basic idea is that the state "does not care" about the individual, which is contrary to the concept of the so called "social-welfare state" that exists both in Slovenia and more or less

in other Member States. Therefore, the concept of data protection in the US is not only contrary to the Slovenian system, but also to the whole EU approach (Europeans Lead US in Data Protection, 1998).

While the US Constitution does not explicitly include the right to privacy, it includes its specific aspects implicitly in some of its Amendments. To name a few examples, the First Amendment touches the privacy of beliefs, Third Amendment protects the privacy of the home against the demands of soldiers and the Fourth Amendment extends to the protection of person's privacy and possessions against unreasonable searches, which is actually more connected to criminal law and not the privacy or data protection laws (Linder, 2023). The US Supreme Court has, however, for decades interpreted the Amendment XIV in a way, to guarantee a broader right to privacy, but namely in cases of marriage, procreation, child raising, and ending of medical treatment (Linder, 2023). Nevertheless, as the right to privacy is not explicitly included in the US Constitution, an established precedence substantiated on the implicit right might easily fall by arguing there is no constitutional basis to stand on.[1] In this consideration, the right to privacy in the US is on shaky fundaments.

The right to privacy in the US system always seems to be a part of some other norm. Therefore, it is beneficial to explore the idea behind the constitutional rights in the US, which at least implicitly include the aspect of the right to privacy. The aspect of the right to privacy is not given in the sense of a positive right, as it is typically set in Europe. The US Constitution is a charter of so-called "negative rights" (Currie, 1986, p. 864). The latter means that its legal framework is not structured in a way that would dictate the state to take care of its citizens. On the contrary, it is based on the concept that the state will not excessively interfere with the individual or his relationships if the Constitution does not suggest otherwise. For example, the Fourteenth Amendment prevents the state from repressing the individual by prohibiting the state (through its bodies and organs) from doing so, not by granting a right to the individual directly (Turnšek, 2024, pp. 51-54). Admittedly, the US added amendments, such as the First Amendment, Third Amendment, Fourteenth Amendment, some even mention the Fifth Amendment, which in side-lines cover the aspects of privacy, but do not necessarily touch the protection of personal data as well. In any case, as observed by academic writers like De Bruin, those additional provisions are dissonant with modern technological development and digitalization and therefore, do not offer sufficient protections for individuals' privacy (De Bruin, 2022 p. 141).

Currently, significant amounts of personal data are being spread through the internet at an unimaginable speed. Healthcare systems, representing one of the

[1] That already happened with the right to abortion, which was given in the decision in Roe v. Wade in 1973, but was recently overruled in Dobbs v. Jackson Women's Health Organization. See: https://www.scotusblog.com/case-files/cases/dobbs-v-jackson-womens-health-organization/ (accessed on 23. 12. 2024).

biggest informational-technological systems in a particular state, are striving to move as much data as possible to online forms. Considering social media, 510,000 comments are posted on Facebook every minute and more than 95 million pictures are posted on Instagram each day (Tzanou, 2020, p. 4). In every sector, increasingly more tasks and documents are being taken from the common physical forms that we knew to various platforms in the e-environment. In his comparative analysis, Ruben de Bruin argues that this individual sharing and processing of personal data dictates data privacy regulation in the US, and sees the US Constitution as a driver of strengthening the rights of data processors, rather than, unfortunately, as a shield to protect the weaker individuals (De Bruin, 2022 p. 141). Schwarz and Peifer share a similar view, linking the internet primarily to consumer's benefits, which in the end results in the creation of great wealth for the US economy (Schwartz and Peifer, 2017, p. 155). With so much emphasis on the economy in the US, the influence of the state on the private sector and on disputes between individuals is quite limited. Interestingly, the newly proposed American Privacy Rights Act of 2024 (hereinafter: APRA),[2] emphasizes the rights of business by including sections on interference with consumer rights (section 107 APRA), service providers and third parties (section 111 APRA) and data brokers (section 112 APRA). Even though the APRA shall represent a unification of the privacy rights across the states,[3] it does not improve the position of consumers. To support the latter, see section 101.13.D APRA, according to which the service providers are excluded from the scope of APRA, thus providing a loophole for numerous entities hypothetically seeking a way for them to skirt the law. Moreover, it may already seem that consumers are given a special protection under section 107 APRA[4], dealing with interference with consumer rights. To the contrary, according to this section the consumers are explicitly protected merely from the entity acting in a so-called "dark pattern" – in a way trying to undermine or impede the user's autonomy, decision-making or choice by users' interface or in case of false, fictitious, fraudulent, or materially misleading representations. Indeed, enacting APRA would help establish a higher standard of privacy protection in the US, while maintaining consistency with their essential views, system and fundamental values. It would be presumptuous to assume the APRA would provide as high level of general protection of personal data as does the GDPR in the EU. Considering all the above, it is no surprise that legislation enacted in the US concerning the rights to personal autonomy,

[2] American Privacy Rights Act of 2024, H.R.8818 - 118th Congress (2023-2024).

[3] If accepted – for now it is not yet at the stage of being implemented.

[4] See the first subsection of Section 107. (Interference with consumer rights), which sets forth the following wording: *»IN GENERAL. A covered entity may not use dark patterns to:*
(A) divert the attention of an individual from any notice required under this title;
(B) impair the ability of an individual to exercise any right under this title; or
(C) obtain, infer, or facilitate the consent of an individual for any action that requires the consent of an individual under this title.«

the protection of personal data, privacy and the dignity of the individual in the US are much less robust (De Bruin, 2022 p. 142) when compared to the EU. From the US perspective, data portability promotes the success of the business and industry, while adding or extending human rights protection would only hinder it. Any restriction on the promotion of progress and innovation would be contrary to their core values and fundamental legal acts, as well as to American society's belief in the benefits of their approach (De Bruin, 2022 p. 142).

The US Constitution and American belief system aside, the US does not have a covering legal act that would govern data protection in general, similar to that of the Slovenian Privacy law (Zakon o varstvu osebnih podatkov, hereinafter: ZVOP-2)[5] or Union's General Data Protection Regulation (hereinafter: GDPR)[6]. Admittedly, the United States do have many legal acts that are related to a specific field of studies and govern data protection within that particular field (Pop, 2023). Their fragmented legislation is constituted on different levels, federal, states and sectoral, and, at the same time, it is composed of a series of laws (Mastracci and Salemme, 2024). There is a more general privacy act, titled US Privacy Act, which is very broad and applies to all US citizens and foreigners with lawfully obtained permanent residence (Mastracci and Salemme, 2024). The APRA in some aspects follows the GDPR. Admittedly, it protects privacy and personal data on the federal level, it proposes additional boundaries for processing of sensitive personal data, sets the similar if not the same principal values such as data minimization, transparency, yet it fails to set out the significant principles of purpose limitation or for instance storage limitation. Even though it specifically mentions the protection of weaker parties – like children and consumers (which are not particularly mentioned in the GDPR), it fails to provide the same level of protection as GDPR and to create higher standards for data protection in more general view. In particular, the Congressional Research Service noted that the APRA would create a comprehensive federal consumer privacy framework,[7] which is very limited to the field of business while GDPR is a more general regulation that covers aspects of data protection (principles and rights, operations, liabilities, remedies, sanctions, types, etc.) as a whole.

If one wants to find the privacy and data protection rights of a specified field of studies in the US, then one must find a federal act that is focused on this particular matter. Let us consider the health sector as an example. In connection

[5] Zakon o varstvu osebnih podatkov (ZVOP-2) Uradni list RS, št. 163/22.

[6] 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).

[7] Congressional Research Service (2024, May 31). The American Privacy Rights Act. [Data file]. Retrieved from https://crsreports.congress.gov/product/pdf/LSB/LSB11161.

with the healthcare sector and patients' rights, the US has a legal act on the federal level, titled The Health Insurance Portability and Accountability Act[8] (hereinafter: HIPAA), which protects patients' sensitive health personal data. HIPPA, similar to the US constitution, does not pay its primary attention to the rights of the patient as much as for example the Slovenian Patients' rights law (Zakon o pacientovih pravicah, hereinafter: ZPacP)[9] does. Importantly, it does protect the privacy of a patient (e.g. the protection of data exchanged between the doctor and a patient); however, it also covers the questions of technical nature regarding the health and life insurances, taxes, even the prevention of healthcare fraud and abuse and more aspects, which may hinder its focus from the more detailed patient's rights protection. Both, ZPacP and HIPAA, cover the matter of healthcare providers obligation to establish a secure system for accessing health information and to comply with the privacy regulations. In the US these regulations are governed by the U.S. Department of Health and Human Services (hereinafter: HHS) (Lutkevich, 2020). That is slightly different from the regulatory scheme of the EU, where the third paragraph of Article 16 of the Treaty on the Functioning of the European Union (hereinafter: TFEU)[10] suggests each Member State should establish a supervising body that examines and censors the respect and protection of personal data in its territory. For instance in Slovenia that body is the so-called Informacijski pooblaščenec (en. Information Officer), in Croatia, the supervising body is Agencija za zaštitu osobnih podataka (en. Croatian Personal Data Protection Agency) and in Italy, the supervising body is Garante per la protezione dei dati personali (en. The Italian Data Protection Authority).

b. The EU concept of data protection

The EU approach regulating the protection of personal data focuses mainly on two goals: to ensure adequate protection of human rights and to enable trade, which requires the exchange, sharing and other types of processing of personal data (Lissens, 2024). In the EU, it has already been expressed that the data subject should be treated as a person and not merely as a consumer or user; such non-personal approach would violate the dignity of the data subject concerned.[11]

[8] HIPAA Administrative Simplification Regulation Text 45 CFR Parts 160, 162, and 164 (Unofficial Version, as amended through March 26, 2013).

[9] Zakon o pacientovih pravicah ZPacP) Uradni list RS, št. 15/08, 55/17, 177/20 in 100/22 – ZNUZSZS; a specific Slovenian legal act, which governs the rights and duties of the patients as well as rights and obligations of doctors and other medical/healthcare employees.

[10] Treaty on the Functioning of the European Union, OJ C 326, 26. 10. 2012.

[11] European Data Protection Supervisor, Opinion 4/2015 Towards a new digital ethics - Data, dignity and technology. URL: 15-09-11_data_ethics_en.pdf (europa.eu) (November 16, 2023).

Admittedly, EU law has a different historical, societal and cultural background as well as different legal fundaments in comparison to the US. All of those components, together with the horrors of World War II, undoubtedly helped pave a different path for the development of law and understanding of the core values, rights and freedoms in today's Member States. In 1950, the European Convention of Human Rights[12] (hereinafter: ECHR), with its Article 8, became one of the first European legal acts advancing the protection of personal data. It successfully (yet indirectly) protected personal data of individuals through the right to respect for private and family life (Article 8 ECHR), which can be confirmed from the extensive case law connected to this particular field (see cases: *Surikov v. Ukraine (2017), Z. v. Finland (1995), Halford v. UK (1997), Biriuk v. Lithuania (2008), Y.G. v. Russia (2022), P. T. v. Republic of Moldavia (2020), Y.Y. v. Russia (2016), Y. Y. v. Turkey (2015)* etc.). With the Lisbon Treaty[13] in 2008, the EU created the Charter of Fundamental Rights of the European Union (hereinafter: CFR)[14] and put it into force as one of its three fundamental or so-called primary legal acts. Among its inclusion of many other fundamental human rights that had already been covered with ECHR, it also introduced an independent right to data protection to EU primary law.

In contrast to provisions of the US Constitution, which as we have seen is short on enumerated rights and instead employs more general terms such as "due process" and "equal protection," the CFR gives individuals "positive rights", and at the same time, it obliges subjects, from private as well as from public sector, who are dealing with processing of personal data, with certain responsibilities and duties (Schwartz, 2013). In comparison to the Fourteenth Amendment to the US Constitution, for example, CFR's protection of individuals seems to be on a higher level, shielding the weaker party in the equation. Besides protecting individuals from the state's interference, it also prevents them from any other person's or their-own interfering (Turnšek, 2024, pp. 51-54). The latter means the individual does not have an "opt-out" option to refuse or deny the right given by the CFR. Indeed, it is a generally accepted fact that fundamental human rights cannot be denied or refused. De Ruben stressed that having the right to refuse such right could undermine the individual's capacity for self-determination (De Bruin, 2022 p. 140). An individual is the master of his own rights – considering the right of data protection, he is in power to decide upon questions in connection to his personal data[15] (De Bruin, 2022 p. 140). The latter is completely opposite to the

[12] European Convention of Human Rights (ECHR), 1950, amended and supplemented by protocols 1, 4, 6, 7, 11, 12, 13, 14, 16.
[13] Lisbon Treaty, OJ C 306/01, 17. 12. 2007.
[14] Charter Of Fundamental Rights Of The European Union, Official Journal of the European Union, OJ C 326/391, 26. 10. 2012.
[15] An individual alone can decide on questions like which data and to what extent should those be processed, in what period will those be processed, by whom and to whom will those be transmitted to etc.

interpretation of the same right and its understanding in the US and it is also contradictory with the whole privacy-concept as understood in America.

Similarly to the US model, however, EU data protection legislation is provided on the EU level as well as in the national legal system of each Member State. EU constitutes the right to data protection in primary EU acts and further on, through its secondary legislation – however, it cannot be considered as fragmented. Directive 95/46/EC (hereinafter: Data Protection Directive)[16],was the first important secondary legal act governing the data protection. The most relevant act of today is the topical GDPR. Both set the universal (minimal) standards of data protection for all of the Member States touching different sectors and fields of studies in the crossroads with the protection of personal data.

Neither jurisdiction should be judged as good or bad. While each preferring its own purpose, goals and generally accepted public interests, the concepts are just very different. In the US, the primary purpose is supporting business and consequently, developing the economy; and in the EU, data protection represents the balance between business and protection of fundamental human right(s), putting the individual as a person in the fore-front. However, because of globalisation and the world-wide market, the distinctions between the two can easily clash and create uncertainty between the two contracting parties, users, service acquirers, buyer-seller or other parties coming from two different legal systems.

3. The development of personal data protection in EU

Since 2018, the most relevant legal act governing this field is GDPR. Although GDPR is probably the most comprehensive and demanding data protection act due to its narrow rules, it is not the first EU act governing data protection in general. In fact, GDPR is a direct successor of Data Protection Directive and indirect successor of The Convention for the Protection of individuals with regard to automatic processing of personal data[17] (hereinafter: Convention no. 108)[18].

[16] 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.

[17] Zakon o ratifikaciji konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, Uradni List RS, št. 11/1994 z dne 28. 2. 1994.

[18] The Convention for the Protection of individuals with regard to automatic processing of personal data and its additional Protocol of the Council of Europe of 28 January 1981, European Treaty Series - No. 108.

a. Convention no.108

Convention no. 108 was the first legally binding act in the field of data protection, made by Council of Europe in parallel timing, but completely separate to OECD's Guidelines (Turnšek, 2024, pp. 1-2). At the time, some European states already had a legal framework in this field (e.g. Germany) while others had none. Ever since, this Convention has been ratified not only by Member States of the Council of Europe, but also by the third-world countries such as Uruguay and Mexico (Turnšek, 2024, pp. 1-2). It was crafted with a purpose to recognise and guarantee the rights to privacy and to data protection as fundamental human rights as well as to strengthen the cooperation between the Member States for the purposes of free flow of information and prevent any misuse or violations (Walter). Such goal could not be reached in a scenario where every state had different legislation with different definitions and measures or no legislation of the field at all. Therefore, Convention no. 108 provided its "states signatories" with common standards of data protection, which are based on internationally recognized basic principles that all signatories follow and are relevant still to this day. However, by now some states or other entities, like the EU, have accepted new data protection regulations.

b. Primary EU law

The EU is *sui generis*, a uniquely structured subject that does not present a country or federation, albeit it unites the Member States and allows them to create legally binding decisions, documents, and legal order. The EU was created and still stands on its primary legal acts – Treaty on European Union[19], TFEU and CFR. Although the EU is recognized for its comprehensive legal order with many regulations, directives, Commission's opinions, precedential case law etc., its primary law constitutes the utmost relevant provisions, which serve as the basis for the rest of its secondary legislation.

Intriguingly, roots of data protection have been injected into the core of the EU legal order in the context of Article 16 TFEU and Article 39 TEU and even more precisely with Articles 7 and 8 of the CFR. Pursuant to Article 16 TFEU, the individual is given a right to data protection, which shall be governed by law accepted through legislative procedure and censored or protected by an independent body. The latter is additionally recognised by the Article 39 TEU. While granting significant importance to data protection law, Article 16 TFEU presents a legal basis for the secondary legal acts in the particular field of studies.

The Articles from CFR are more specific than the mentioned provisions of the Treaties, but still broad enough to establish a basis for this field and its

[19] Treaty on European Union, Official Journal of the European Union, OJ C 326/01, 26. 10. 2012.

protection. Article 7 CFR, identically to Article 8 ECHR, establishes the right to privacy in private and family life, home and telecommunications. Further, Article 8 CFR sets forth the direct right to data protection, and recognizes the importance of processing of personal data, which has to be fair, executed for a specific, limited purpose, on a particular legal basis and it has to be accessible to the individual these data concern.

Admittedly, these are the basic provisions that outline this rapidly evolving field of law. In this regard, data protection must be regulated further on with secondary legal acts, such as directives or regulations.

c. Data Protection Directive

In 1995, the EU harmonized this legal field among its Member States with a Data Protection Directive. Practically, it was inevitable for the EU to leave data protection law untouched, as regulation of transmitting, storage, use and processing of data is essential for the free movement of goods, capital, services and people within the EU's internal market. This directive provided detailed rules and additional obligations of an independent regulatory authority. Importantly, it was based on the right to privacy, which is in legal theory considered as a much broader right then the right to data protection. With all the technological, software and information-systems' development since the year 1995, the right to personal data has become a very topical and endangered right. One of the precedential cases, confirming the previously stated is Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González[20].

Mr Costeja González, a Spanish citizen, lodged two complaints against La Vanguardia Ediciones SL, a daily newspaper publisher with a large circulation, and against Google Spain and Google Inc. More than ten years prior to this proceeding, Mr González had some problems, resulting in a real-estate auction to recover his social security debts. Because of the pattern of Google's search engine, every internet user that entered Mr Costeja González's name in a Google Search found the links to two pages of posting about his social security debts and auction, even though those matters were fully resolved years ago and were now completely irrelevant. By lodging his complaints, Mr Costeja González requested two issues to be resolved. First, that La Vanguardia remove or alter those pages so that the personal data relating to him no longer appeared or to use certain tools by search engines to protect his data. Second, he requested that Google Spain or Google Inc. remove or conceal the personal data relating to him so they would no longer appear in the links to La Vanguardia. His complaint against La Vanguardia Ediciones was rejected, on the grounds that the Spanish Ministry of Labour and Social Affairs had ordered an announcement of this auction in this very journal, because the goal was to

[20] Case C-131/12.

attract as many bidders as possible. However, the complaint against Google Spain and Google Inc. was upheld. Google Spain and Google Inc. challenged this decision before their National High Court, which finally asked the Court of Justice of the European Union (hereinafter: CJEU) for a preliminary ruling regarding three issues. First, the CJEU confirmed that this case lays within the scope of the Personal Data Protection Directive. In connection with the second question, the CJEU stressed that the activity of a search engine should be understood as "processing of personal data" when the information delivered by the search engine contains personal data. Unsurprisingly, the CJEU specified that the one operating such search engine represents the controller. As an explanation for the third part of the preliminary ruling, the CJEU stated that inadequate, irrelevant or excessive data might not be compliable with the provisions of the Personal Data Protection Directive. In other words, if the data is inadequate, irrelevant or excessive, such information and links in the list of the results should be erased. After the CJEU published this decision, many similar stories came to the surface. This ruling was followed by a burning public debate, resulting in the formally accepted "right to be forgotten" in Article 17 GDPR later on.

The purpose of outlining this whole case was to show the number of unregulated questions and loopholes and with that, to substantiate why the Data Protection Directive became insufficient. It not only failed include the rules crafted within the precedence's of the CJEU and ECtHR (as in the mentioned case), but it also had slowly started losing its relevancy and accuracy according to technological developments. Importantly, although the Data Protection Directive was purposely intended to protect individuals against the inappropriate use of information technology, it was not designed to prevent the processing of such information or to limit the use of information technology as such (Hustinx, 2014). In other words, its purpose was to ensure people with certain rights in the digital world, without a particular focus on data relating to the concerned individual. However, in the modern age data protection per se is of great importance. The EU realised the latter and started creating another, more relevant legal act in 2012. The GDPR was finally confirmed and accepted in 2016, but entered into force in 2018 – that is when the Data Protection Directive was finally invalidated.

d. General Data Protection Regulation through comparison with the mentioned documents

There are important distinctions between the Data Protection Directive and GDPR. The directive harmonizes legal orders of Member States, which means that it only sets forth the rules, without including the ways in which those should be implemented (there is not only one way, because every Member State adapts it in the light of its own legal order and its needs). On the contrary, the GDPR unifies the legal orders of Member States, meaning the regulation applies to every Member State directly. As the GDPR is binding for the Member States,

it is also binding in the United Kingdom (on the basis of Withdrawal Act 2018[21]) and in three states from the European Economic Area (Norway, Iceland and Liechtenstein).[22] Moreover, its effect expands extraterritorially, which reflects through its applicability outside of the EU, EEA and United Kingdom. That is possible if one of the two situations arises: if a person who is on the territory of EU/EEA is offered some service or goods from a person outside this area, and if a person's behaviour is being monitored when he or she remains on the territory of EU/EEA (e.g. regularly or in intervals checking an individual's location).[23] It is significant that the person, who is being offered goods, service or is being monitored, remains in the territory of EU/EEA and it does not matter which citizenship this person possesses.

Territorial scope aside, the GDPR also extends its material scope. From Convention no. 108's applicability to automated personal data files and automatic processing of personal data in the public and private sectors[24], the GDPR applies to the processing of personal data by automated means as well as to the processing of personal data which form (or are intended to form) part of a filing system[25]. The new definition emphasizes four key points, serving as requirements, which have to be fulfilled for the GDPR to apply.

First, the personal data must be processed. Processing is defined very broadly and includes any type of use, change, storage, rectification, transmission or similar activity concerning personal data. Second, the personal data must belong to a natural person; a company or other legal entity fails to qualify. Considering the fact that Convention no. 108 included a company or other legal entity and that the Data Protection Directive did not reject nor deny it, the GDPR made a hard turn by excluding such possibility.[26] Additionally, to qualify a natural person has to be identified or at least identifiable, which means that we may recognize this individual by this particular data without acquiring some additional more extensive costs, time or input.[27] The third condition requires presence of some kind of technology – whether that is a server or for example a computer. Lastly, the provision requires this data to be a part of a

[21] UK Government, »European Union (Withdrawal) Act 2018 (c. 16).«
[22] European Data Protection Supervisor, »Cooperation with European Economic Area (EEA) and European Free Trade Association (EFTA).«
[23] Article 3 (2a) (2b) GDPR.
[24] Article 3.1 Convention 108.
[25] Article 2.1 GDPR.
[26] In comparison, Convention no. 108 included an extra option. Article 3(2b) of the Convention no.108 provides that any signatory applies this legal act and its rules to legal persons too. The State was given an option to provide a notice addressed to the Secretary General of the Council of Europe declaring it will extend the content to legal persons. A few examples of States that chose this approach are Austria, Italy, Liechtenstein, Switzerland, etc. Recital 24 Directive 95/46/EC explicitly stated that extending personal data regulations to legal person is not contradictory to this directive. GDPR has taken a different stand.
[27] Introductory provision 26 GDPR.

collection of data with a certain structure, on the basis of which particular data can be found. Such filling system can be in a condensed form or spread over a series of different places. The point is that because of this structure particular data of a specific person may be found.

In comparison to the Data Protection Directive and Convention no. 108, the GDPR provides the strictest standards so far, more detailed rules and for some violations much higher financial sanctions. Details can be found in Articles 83, 84, 151, 154 GDPR.[28] Notably, the GDPR has set higher standards regarding the explicit consent and the duty to inform.[29] The latter is of significant importance, especially in the system we live in now because hospitals, institutions dealing with sensitive personal data, are full of elderly – digitally illiterate people and health apps are equipped with complex Privacy policies and other typical contracts. The evolution of data protection introduced by the GDPR can be seen not only through re-defined terms and added definitions, but also through added provisions regarding complex relations between controller and processor, joint controllers, and the controllers' need for Data Protection Impact Assessment before personal data and like information is processed.[30]

4. Defining personal data

Data protection derives from the broader right of privacy, and possibly from the core human right of dignity (Turnšek I, 2024, p. 94). However, to understand the legal field, we must first clarify the basic definition of *personal data*. In one of its decisions, the CJEU explained that if a person can be identified (without additional costs, time and effort) by particular data, then these data count as personal data.[31]

Pursuant to Article 2(a) of Convention no.108, the definition of personal data stands for "information relating to an identified or identifiable individual ("data subject")".[32] Article 2(a) of the Data Protection Directive defined the term

[28] Article 83 suggests general conditions for imposing administrative fines and describes various factors, which may influence the final amount of the fine. Administrative fines can – e.g. if the controller's or processor's breach is detrimental - reach 10 million euros or 2 percent of the total worldwide annual turnover of the preceding financial year; or – e.g. if the subject does not compy with an order of supervisory authority – 20 million euros or 4 percent of the total worldwide annual turnover of the preceding financial year.

[29] Pursuant to Article 7 GDPR, an individual must be informed of the risks in an understandable and easily accessible form and in clear and plain language.

[30] See cases: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH (2018), Google Spain SL, Google Inc. protiv Agencia Española de Protección de Datos (AEPD), Mario Costeja González, (2014), Jehovah's witnesses v. Finland (2023).

[31] Case C-582/14.

[32] Article 2(a) of Convention no. 108.

almost identically but added a part, explaining "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factor specific to his physical, physiological, mental, economic, cultural or social identity". The latest and today's most relevant definition of personal data is laid down in Article 4(1) GDPR. There, personal data is again defined nearly the same as in the Data Protection Directive, but with additional possible identifiers "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".[33] Interestingly, personal data has kept the same core meaning since 1981. The definition suggests that personal data should be related to a natural person (only Convention no.108 held an option to project that onto legal persons too), who is alive and who is or can be identified by this particular information or identifier. The qualificators that are legally set forth are important; however, the mere purpose of collecting certain personal data has a great significance as well and has to be taken into account.[34] Moreover, the CJEU stressed that the aim of this provision is to be interpreted broadly, to be able to potentially cover all types of information – both objective and subjective, in various forms – as opinions or judgments, as long as they relate to the person concerned.[35]

Although the culture and society have quite drastically changed and technologies developed significantly since then, the basis remained and only new specific factors, identifiers have been added. From my personal point of view, these additions are an important asset, because they bound the pool of information that can count as personal data in accordance with social and technological development. Additionally, if a specific factor refers to a characteristic or quality of an individual in a way that might be discriminatory, then processing the personal data is prohibited (unless it falls into one of the exceptions under Article 9(2) GDPR). Personal data that disclose racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation are considered as a special category or sensitive data and are therefore highly protected.[36]

[33] Article 4 GDPR.
[34] UPRS I U 1079/2012.
[35] Case C 479/22.
[36] Article 9 GDPR.

5. Sensitive data with an emphasis on health data

Regarding personal data in relation to one's racial origin or sex life, it is more likely for it to represent a basis for discrimination, then e.g. information about one's job or the faculty this individual finished. Looking from both – cultural and historical point of view – these very intimate personal beliefs (e.g. political or religious) and characteristics (such as person's physical appearance, attractiveness to women or men, invalidity etc.) were considered to be "correct" or "socially acceptable" if preserved in a certain way, otherwise individual's opinion or behaviour was quickly seen as wrong or weird. To be more dramatic, in the Middle Ages women who were smarter or considered to be open-minded were labelled as witches, conquistadores saw Indians and black people as slaves and babies born with disabilities were in many cases rejected as god's punishment or considered cursed. Even today, society still sees particular groups of people or their particular characteristics differently in a negative way. According to the highest human rights' legal acts, pursuant to Article 2 TEU, Article 14 ECHR, Article 1 and 2 the Universal Declaration of Human Rights (hereinafter: UDHR)[37], discrimination of any kind is prohibited. Even so, discrimination still occurs.

Interestingly, law usually prohibits discrimination in a broad way, without laying down the narrower definitions or explanations of certain terms. When it comes to understanding the meaning of racial origin, there is no confusion regarding its meaning. On the other hand, "data concerning health" does not provide the reader with a clear term or definition. Does it cover only the basic health problems, such as breaking a leg or catching a virus? On the other hand, does it include mental health problems, being diagnosed with various disorders or rare immune disease? If focusing particularly on the data concerning health for example, we can easily see its scope cannot be defined just by reading the GDPR, as it does not provide a more detailed description of the term. In the case of Mrs. Bodil Lindqvist[38], the CJEU provided a ruling in which it directly addressed the dilemma on whether data concerning health should be interpreted widely. Answering affirmatively, the CJEU confirmed such data include information concerning both, physical and mental aspects of an individual's health and emphasized the importance that health data be given a broad interpretation.

Further, the term "health data" is not limited merely to the information, circulating through the healthcare systems or the information in doctors' files. Health data more broadly subsumes all the health-related information in virtual environments, such as information of our sleep quality provided by our personal smartwatch, the number of steps in a day collected by our smart phone, or data put in any health or sports app on our phones, computers or smartwatches. Unfortunately, these data are not always safely saved and waiting for a

[37] United Nations General Assembly. The Universal Declaration of Human Rights (UDHR), 1948.
[38] Case C-101/01.

concerned individual to add some new data. To the contrary, these data are being collected, and in some cases used, advertised or even sold to others by the app provider. Frankly, consumers are not keen about reading privacy policies and terms and conditions before entering such apps. Consequently, they are frequently completely unaware of their data being processed, even though they clicked they agree with it. That is particularly concerning in cases where the data being processed represents health data – one of the most sensitive groups of data, reaching a very intimate sphere of individuals' personal and family life. Unfortunately, there are already some cases in which such practice was discovered (for instance BetterHelp, which is deliberated later on).

Mozilla Foundation, a non-profit organization, studied some of the most popular period-tracking and pregnancy-tracking apps. Shockingly, it found that 18 out of 20 of those raised some concerns in the field of privacy or security (Masunga, 2022). Ovia, an American pregnancy-tracking app, provides a case in point. Ovia's app is supposed to be consistent with HIPAA or "other privacy laws" (Ovia, 2024). However, when an EU citizen or person, who remains in the EU, tries to enter and log-in to the app, it does not mention any applicability of the GDPR or respect towards its provisions. As a precondition when logging in to the app, the user must agree both with its Privacy policy and Terms of Use has and must also consent to "Ovia's processing of personal data in the US, including data about his health, fertility, pregnancy, sex life and family circumstances, to customize and improve Ovia services".[39] The latter may count as an explicit consent pursuant to the GDPR, which is an obligatory basis for lawful processing of sensitive personal data.[40] Without agreeing to the foregoing, the user cannot enter into the app or use it in any way. In their Privacy policy, they list many health data, which Ovia collects – from basic ones, including hours of sleep, height, weight, to more intimate ones, such as number of weeks pregnant, the trimester, fertile window, information about the user's children, health insurance information, employer and employee ID, geolocation and more. Additionally, Ovia+, which is a premium version of this app, can be given as a benefit from users' health insurer or employer, and in such case the user's employer may also have access to the given personal data if the user does not explicitly turn off this option (Mozilla Foundation, 2024). Ovia's Terms of Use document lists a number of activities for which the collected data may be used solely for external and internal marketing purposes, analytics or even research, among which sharing these data with the user's insurer or employer is not excluded. On the contrary, Ovia may also sell, lease or lend aggregated personal information to third parties and share collected data with Facebook (The Washington Post, 2024). There are many potential risks if sharing of such data occurs – from the user losing a job or not being promoted because of trying to conceive a baby, to being rejected from a particular

[39] Citation of one of the requirements when logging in Ovia.
[40] Article 9 GDPR.

insurance package or premia for instance. In a very recent case, the ECHR explained that security services' direct access to the data stored without adequate safeguards against abuse and the requirement to decrypt encrypted communications cannot be regarded as necessary in a democratic society as it impairs the very essence of the right to respect for private life under Article 8 ECHR.[41] In parallel, we can see the analogy with the Ovia case. The ECHR ruled so in the case concerning internet communications and its users, but Ovia is dealing with extremely intimate health data and uses them for marketing, analytics purposes and even for "improving their services", without defining what that means. The Mozilla Foundation published an article about those loopholes in 2022. Even today, there are no additional references to the GDPR, or measurements taken in the sense of additional efforts or safeguards for the protection of users and their sensitive data. Although the ECHR may not apply to a US company directly, it should apply if it was being used by a person in the territory of the EU and vis-a-vis, there is no legal order, according to which Ovia's activities could be classified as "necessary in a democratic society".

From my point of view, the biggest loophole in the system is not even in the legislation itself, but rather in unfair business practices. Admittedly, the app provider is from the US, which means they will follow the US concept of the right to privacy and consequently put more efforts into developing business and earning a fortune, then into protecting human rights, individual's dignity, privacy and basically their private lives. The first major error in this case is having such app on a worldwide market, while simultaneously failing to acknowledge the most challenging privacy act, the GDPR. If the data is collected from the individual, who remains on the territory of the EU, then the GDPR applies. In other words, the Ovia's data controller and processor are obliged to follow the concept of protecting the weaker parties, which are in this case users, as well as to respect the relevant provisions of the GDPR. Therefore, even if the app provider belongs to a Non-EU legal system, when it clashes with the territory of the GDPR, it has to refrain from the US or another concept and apply provisions of the GDPR's. The second major inconvenience, which at the same time represents a much broader problem that modern society is facing, is the form of consent given when conducting typical contracts. While users click the "I agree" button and providers of services or goods accept the given consent as if everything was fully understood, agreed with and accepted with clarity, knowing it was not, we are presented with a paradox. The argument that users could read the terms of consent is also deficient, because people without a legal background cannot understand most terms. Presently, typical contracts are conducted frequently and not only through virtual platforms (but also in physical stores – providers of technological equipment and goods use them all the time), but e-environment certainly does in many cases make business slightly less transparent.

[41] Case of Podchasov v. Russia (2024).

However, Ovia is not the only app suffering from a lack of privacy and data protection. In 2021, Macquarie University of Australia produced an extensive research on mobile health and privacy. It included almost 21,000 health, medical and fitness apps (Tangari et. al., 2021, p. 1). Intriguingly, 88.0 percent of those health-related apps included code that could potentially collect user data and 28.1 percent of them provided no privacy policies (Tangari, et. al., 2021, p. 1). Another study, focusing particularly on the privacy of mental health apps (Iwaya, et. al., 2023), revealed even more issues regarding the lack of privacy concerning data protection. In an empirical investigation and its implications for app development, researchers found unnecessary permissions, insecure cryptography implementations, and leaks of personal data and credentials in logs and web requests (Iwaya, et. al., 2023). Furthermore, these researchers highlighted the high risk of user profiling, as the apps' development did not provide fool proof mechanisms against detectability and identifiability (Iwaya, et. al., 2023). That is especially concerning respecting highly sensitive information, such as mental health diseases, biometric data and fertility or other gynaecological issues. These deficiencies may have far-reaching, negative consequences resulting from leaking sensitive data to either the public or particular groups of people (e.g. co-workers) that have the power to turn one's life around. Both the ECHR and the CJEU have dealt with a number of cases where victims were the subject of data breaches resulting in stigmatization, family problems, job loss, social exclusion, etc.[42]

In a recent case, the US Federal Trade Commission (hereinafter: FTC) alleged that the BetterHelp app, which deals with online counselling for particular groups of people (e.g. Pride Counselling for members of the LGBTQ+ community, Faithful Counselling for people of Christian faith, Teen Counselling for teenagers with parental permission), led to serious data breaches versus their clients. The FTC argued that the company repetitively pressed people to respond to questionnaires demanding their sensitive health data, without asking them to consent or showing the respondents their privacy policies at the outset (Fair, 2023). Although BetterHelp assured clients the provided answers and information would be kept private, to the contrary it shared the information with major advertising platforms, such as Facebook, Snapchat and Pinterest. To draw a better picture, BetterHelp allegedly uploaded the email addresses of all its clients at the time, which included nearly two million people, to Facebook to send them adds, get referrals to their friends etc. (Fair, 2023). These tactics resulted in bigger profits for BetterHelp and expanded their clientele, at the expense of a great number of individuals who suffered serious data breaches. Yet again, such an approach goes hand-in-hand with the American concept of the right to privacy, which is constantly undermined by business development and its profits. Approximately one year later, the FDT finally reached a settlement with BetterHelp in May 2024. The

[42] See cases: Z. v. Finland (1995), Y.G. v. Russia (2022), Y.Y. v. Turkey (2015), Surikov v. Ukraine (2017) etc.

terms of settlement called for a 7.8-million-dollar payment, from which people whose rights were violated received their refunds (Federal Trade Commission, 2024). The problem, however, is that mere refund payments can not undo the irreparable harm caused by the wrongful disclosure of one's private information.

It could be concluded that in this case not only the rights to data protection and privacy were violated, but also the impacted individuals' right to dignity. Notably, the ones using mental health apps use them with a certain purpose – to obtain some kind of mental help. Mental health problems are often misunderstood, followed by judgmental opinions, bullying, stigmatizations or even social exclusions. Thus, such privacy violations and data protection breaches on mental health platforms could (instead of improving) cause worsening of vulnerable individual's health condition. For this reason, health-related apps should have been forced to develop and implement even stricter privacy policies and stronger data protection systems in comparison to other mobile and computer apps created for entertaining, business, communication or for example artistic purposes. Such companies with high number of users should also go further and protect data with pseudonymisation or anonymisation of data. As information technology is so advanced and developed, it is unfortunate to see how it is being exploited for profits, marketing and business at the expense of fundamental human rights.

6. Conclusion

To sum it up, there are major differences between the interpretation of the right to data protection in the US and EU legal systems. Their fundamental views on privacy of individual and protection of personal data differ in the very core understanding of the right to privacy. According to the EU concept, the primary focus is the protection of the fundamental human right to a private personal and family life. It is of utmost importance to keep everyone, the state and other individuals, private companies, governmental and non-governmental bodies, from interfering with an individual's privacy. On the other hand, the ideology of the right to privacy from the American legal system deviates from the EU concept. It neglects the human rights aspect, emphasizing instead the betterment of business and the economy. Because the American concept highlights the principle of the individual being "left alone", the individual is literally being left alone, not getting the additional protection that he should be given according to the basic human right's legal acts, for instance, see Articles 1 and 2 UDHR, Articles 7 and 8 CFR or Article 8 ECHR. Admittedly, the proposed APRA (should it be adopted into law) would be a great contribution to the development of the privacy protection in the US and it would guarantee a higher level of protection than the Americans have now. It specifically proposes some particular provisions focusing on specific groups. For instance, it provides the protection for children's privacy in particular, as well as personal data, which is a step forward or even a step ahead of GDPR. However, it is

questionable if its protection of personal data will in general view be at the same level as the protection according to GDPR (taking into account APRA's missed principles – fairness, accuracy, accountability, storage limitation, that are included in the GDPR, controller and processor's checks and boundaries such as data protection impact assessment pursuant to GDPR, the need for adequacy decisions, certificates, having independent supervisory authorities in practise etc.). With a new Congress in the United States, and a new President, the fate of the proposed APRA is in a state of flux.

When such distinctions happen, it is probably the simplest path to return to the basic legal principles and rules. The latter are usually laid down in the fundamental legal acts, for instance ECHR or UDHR. In the EU these would also be the Treaties (Treaty on European Union and Treaty on the Functioning of the European Union) and in US, that would be the US Constitution. These acts represent the basic rules for successful functioning of modern democratic societies. For instance, without the respect of fundamental human rights we cannot really talk about modern civilized society. We can find their interpretations in comprehensive case law of ECHR, CJEU, and the US Supreme court. As we found some parallels in the case of Podchasov v. Russia[43] and Ovia, I believe such similarities could be found in more cases. Even if a particular corporate subject declares its compliance with certain US legal acts, that does not mean it is in any way allowed to violate the right of privacy or data protection or any other human right of one or more individuals.

As the world is becoming greatly globalised, it is becoming increasingly more difficult to draw clear lines between the certain businesses and legal systems. In other words, there are many companies that conduct business online or across the world in various states, which have different legal systems. In this context, the companies should change their privacy policies and terms of conditions according to the relevant legal acts, effective in the countries where they are conducting business. However idealistic or aspirational this may be, in practise, that is not always the case. Many apps together with their providers, even those who deal with very sensitive, intimate health data of great number of people, do not necessarily deliver sufficient data protection to its users. Sometimes not even the minimal standards are reached. In some cases, the reason for this can be explained by poorly written privacy policies and terms of use. In other cases, the national legislation that a certain company or app complies with does not provide sufficient protection for some users from another state according to the much stricter national legal order that provides for higher privacy and data protection standards. Such situation may arise if a US provider sells its services or goods to the individual who remains on the territory of the EU, where the GDPR applies. The US health apps, offering their services in the EU – to the EU citizens, should therefore provide the highest level of data protection and privacy consistent with the GDPR. In reality, European app users are being

[43] Case of Podchasov v. Russia (2024).

pressured to consent to privacy policies that usually imply the applicability of American legislation or their own terms of use, which are also based on the present American legislation – the legislation valid before the enactment of the aforementioned APRA as this act is not (yet) accepted – which leads to low privacy protection. If users do not agree with that idea, in most cases app providers do not provide another option, but decline the use of that particular app. These tactics are not only inconsistent with fair business practises, but contravene the whole purpose of consent as well. Moreover, it could be interpreted as misleading and manipulative for the users that in most cases do not realize they consented to the lower data protection regulations than they are entitled to. Yet again, the users tend to click "I agree" button quite quickly and make app providers work lawful by giving an explicit consent. Even though American APRA provides a certain standard of protection of personal sensitive health data, many health apps on the market right now do not comply with its provisions, because it is only a draft and not yet a binding bill.

In conclusion, no matter what legal act applies, human rights should not suffer because of it but should be respected in their full capacity.

References

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

Baumer, D. L., Earp, J. B., & Poindexter, J. C. (2004). Internet privacy law: A comparison between the United States and the European Union. *Computers & Security, 23*(5), 400–412. Retrieved from http://dx.doi.org/10.1016/j.cose.2003.11.001

Charter of Fundamental Rights of the European Union. (2012). Official Journal of the European Union, OJ C 326/391, 26 October.

Congressional Research Service. (2024, May 31). *The American Privacy Rights Act* [Data file]. Retrieved from https://crsreports.congress.gov/product/pdf/LSB/LSB11161

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol. (1981). European Treaty Series - No. 108.

Currie, D. P. (1986). Positive and negative constitutional rights. *University of Chicago Law Review, 53*(3), 864. Retrieved from https://chicagounbound.uchicago.edu/uclrev/vol53/iss3/4

De Bruin, R. (2022). A comparative analysis of the EU and U.S. data privacy regimes and the potential for convergence. *Hastings Science and Technology Law Journal, 13*(2), 140–142. Retrieved from https://repository.uchastings.edu/hastings_science_technology_law_journal/vol13/iss2/4

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. (1995).

European Convention on Human Rights (ECHR). (1950). Amended and supplemented by Protocols 1, 4, 6, 7, 11, 12, 13, 14, and 16.

European Data Protection Supervisor. (2015, September 11). *Opinion 4/2015: Towards a new digital ethics - Data, dignity and technology* [Data file]. Retrieved from https://www.edps.europa.eu/sites/default/files/publication/15-09-11_data_ethics_en.pdf

European Data Protection Supervisor. (2024). *Cooperation with European Economic Area (EEA) and European Free Trade Association (EFTA).* Retrieved from https://www.edps.europa.eu/data-protection/our-work/cooperation-eu-dpas/cooperation-european-economic-area-eea-and-european-free-trade-association-efta_en

Europeans lead US in data protection. (1998). *Government Computer News, 1.*

Fair, L. (2023, March 3). FTC says online counseling service BetterHelp pushed people into handing over health information – and broke its privacy promises. *Federal Trade Commission.* Retrieved from https://www.ftc.gov/business-guidance/blog/2023/03/ftc-says-online-counseling-service-betterhelp-pushed-people-handing-over-health-information-broke

Federal Trade Commission. (2024, May 6). *BetterHelp customers will begin receiving notices about refunds related to a 2023 privacy settlement with FTC.* Retrieved from https://www.ftc.gov/news-events/news/press-releases/2024/05/betterhelp-customers-will-begin-receiving-notices-about-refunds-related-2023-privacy-settlement-ftc

HIPAA Administrative Simplification Regulation Text. (2013). 45 CFR Parts 160, 162, and 164 (Unofficial Version, as amended through March 26).

Hustinx, P. (2024, September 15). *EU data protection law: The review of Directive 95/46/EC and the proposed general data protection regulation.* European Data Protection Supervisor. Retrieved from https://www.edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en

Iwaya, L. H., et al. (2023). An empirical investigation and its implications for app development. *Empirical Software Engineering, 28*(2). Retrieved from https://doi.org/10.1007/s10664-022-10236-0

James, M. C. (2014). Comparative analysis of the right to privacy in the United States, Canada, and Europe. *Connecticut Journal of International Law, 29*(2), 257. Retrieved from

https://repository.uchastings.edu/hastings_science_technology_law_journal/vol13/iss2/4

Linder, D. (2023). The right of privacy: Is it protected by the Constitution? *Exploring Constitutional Conflicts.* Retrieved from http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html

Lisbon Treaty. (2007). Official Journal of the European Union, OJ C 306/01, 17 December.

Lissens, S. (2024, January 30). The foundations of EU personal data protection law: Privacy and human dignity. *EU-RENEW Blog Series.* [Web blog post]. Retrieved from https://eu-renew.eu/the-foundations-of-eu-personal-data-protection-law-privacy-and-human-dignity/

Lutkevich, B. (2020, August 28). HIPAA (Health Insurance Portability and Accountability Act). *TechTarget.* [Web blog post]. Retrieved from https://www.techtarget.com/searchhealthit/definition/HIPAA

Mastracci, M., & Salemme, T. A. (2024). The evolution of the right to privacy between Europe and the United States. *Swiss Chinese Law Review Journal.* Retrieved from https://scla.world/the-evolution-of-the-right-to-privacy-between-europe-and-the-united-states/

Masunga, S. (2022, August 18). How data from period-tracking and pregnancy apps could be used to prosecute pregnant people. *Los Angeles Times.* Retrieved from https://www.latimes.com/business/story/2022-08-17/privacy-reproductive-health-apps

Mozilla Foundation. (2022, August 9). *Ovia pregnancy.* Retrieved from https://foundation.mozilla.org/en/privacynotincluded/ovia-pregnancy/

Ovia. (2024, September 15). *Privacy policy.*

Pop, C. (2023, November 15). EU vs US: What are the differences between their data privacy laws? *Endpoint Protector.* Retrieved from https://www.endpointprotector.com/blog/eu-vs-us

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). (2016).

Schwartz, P. M. (2013). The EU-US privacy collision. *Harvard Law Review, 126*(7), 1974–1975.

Schwartz, P. M., & Peifer, K. N. (2017). Transatlantic data privacy law. *The Georgetown Law Journal, 106*(115), 155.

Tangari, G., et al. (2021). Mobile health and privacy: Cross-sectional study. *BMJ, 373*(1248), 1. Retrieved from http://dx.doi.org/10.1136/bmj.n1248

The Washington Post. (2019, April 10). *Is your pregnancy app sharing your intimate data with your boss?* Retrieved from https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/

Treaty on European Union. (2012). Official Journal of the European Union, OJ C 326/01, 26 October.

Treaty on the Functioning of the European Union. (2012). Official Journal of the European Union, OJ C 326, 26 October.

Turnšek, E. (2024a). Varstvo osebnih podatkov kot temeljna človekova in pacientova pravica. *Master thesis.* [Master thesis, E. Turnšek]. Digital Library of the University of Maribor. Retrieved from https://dk.um.si/IzpisGradiva.php?lang=slv&id=89430

Turnšek, E. (2024b). The right to privacy and data protection in European healthcare systems with an emphasis on the relevant case law and European legislation. *Medicine, Law and Society, 17*(1), 94. Retrieved from https://doi.org/10.18690/mls.17.1.89-108.2024

Tzanou, M. (2020). *The GDPR and (big) health data: Assessing the EU legislator's choices.* Routledge. SSRN.

UK Government. (2018). European Union (Withdrawal) Act 2018 (c. 16). Retrieved October 2, 2024, from https://www.legislation.gov.uk/ukpga/2018/16/introduction/enacted

United Nations General Assembly. (1948). The Universal Declaration of Human Rights (UDHR).

Walter, J. P. (n.d.). The role of Convention 108 in the international cooperation [Data file]. Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b2a2f

Warren, S. D., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review, 4*(5). Retrieved from https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Zakon o pacientovih pravicah (ZPacP) [Law on Patient Rights]. (2008). Uradni list RS [Official Gazette of the Republic of Slovenia], Nos. 15/08, 55/17, 177/20, and 100/22 – ZNUZSZS.

Zakon o ratifikaciji Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov [Law on the Ratification of the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data]. (1994). Uradni list RS [Official Gazette of the Republic of Slovenia], No. 11/1994, 28 February.

Zakon o varstvu osebnih podatkov (ZVOP-2) [Personal Data Protection Act]. (2022). Uradni list RS [Official Gazette of the Republic of Slovenia], No. 163/22.

Case law

Biriuk v. Lithuania, app. no. 23373/03 (ECtHR, 25 November 2008).
Case C-101/01, *Bodil Lindqvist* (Judgment of the Court of 6 November 2003), ECLI:EU:C:2003:596.
Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (Judgment of the Court of 13 May 2014), ECLI:EU:C:2014:317.
Case C-479/22, *OC v. European Commission* (Judgment of the Court of 7 March 2024), ECLI:EU:C:2024:215.
Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland* (Judgment of the Court of 19 October 2016), ECLI:EU:C:2016:779.
Halford v. United Kingdom, app. no. 20605/92 (ECtHR, 25 June 1997).
P. T. v. Republic of Moldova, app. no. 1122/12 (ECtHR, 26 May 2020).
Podchasov v. Russia, app. no. 33696/19 (ECtHR, 13 February 2024).
Surikov v. Ukraine, app. no. 42788/06 (ECtHR, 26 January 2017).
UPRS I U 1079/2012 (Judgment of 14 May 2014).
Y. G. v. Russia, app. no. 8647/12 (ECtHR, 30 August 2022).
Y. Y. v. Russia, app. no. 40378/06 (ECtHR, 23 February 2016).
Y. Y. v. Turkey, app. no. 14793/08 (ECtHR, 10 March 2015).
Z. v. Finland, case no. 22009/93 (ECtHR, 28 February 1995).