CHILDREN'S RIGHT TO PRIVACY IN THE VIRTUAL WORLD OF APPS

SUZANA KRALJIĆ,[1] EMA TURNŠEK[2]

[1] University of Maribor, Faculty of Law, Maribor, Slovenia
suzana.kraljic@um.si
[2] University of Miskolc, Faculty of Law – Deak Ferenc Doctoral school & Central European Academy, Budapest, Hungary
ema@turnsek.com

The world has become increasingly globalized, with the exchange of goods and services spanning continents, often leading to clashes between differently regulated legal systems. A prominent example of such a conflict arises in the context of digital health applications and the processing of personal data within them. Although in the sense of human rights, the rights to privacy and data protection are guaranteed to every person with numerous national and international legal acts, and secondary law and sectoral legislation that delves into this field. In Europe, personal health data are mainly regulated with GDPR, whereas in US the field is fragmented and regulated by sectoral regulations. The issue occurs when we deal with the protection of personal health data in the virtual world of health apps, which in the US remains in the grey zone without proper legal safeguards. US HIPAA, which governs personal health data at the federal level, does not protect all data provided to a health app, not even data provided to unlicensed counsel offering services through it.

DOI
https://doi.org/10.18690/um.pf.8.2025.11

ISBN
978-961-299-056-5

Keywords:
child's privacy, age limitation, informed consent, personal data and health applications, digitalisation

University of Maribor Press

1 Introduction

The right to privacy today represents a fundamental human right and, by extension, a child's right. The right to privacy falls under civil and political human rights and is defined as such in the most important international human rights treaties. This is, for example, reflected in the Universal Declaration of Human Rights[1] (hereinafter: UDHR)[2], the International Covenant on Civil and Political Rights[3] (hereinafter: ICCPR)[4], the European Convention on Human Rights[5] (hereinafter: ECHR)[6], the Charter of Fundamental Rights of the European Union[7] (hereinafter: CFREU)[8], as well as the Constitution of the Republic of Slovenia[9] (hereinafter: CRS).[10]

The right to privacy is also enshrined in the Convention on the Rights of the Child[11] (hereinafter: CRC). The CRC defines the child's right to privacy in Article 16:

> *»1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.*
>
> *2. The child has the right to the protection of the law against such interference or attacks.«*

Article 16 of the CRC affirms the child's right to privacy, including informational privacy, personal and spatial privacy, and the right to solitude. It also emphasizes the right to protection from arbitrary or unlawful interference with the child's family,

---

[1] Universal Declaration of Human Rights: Uradni list RS, št. 24/18.
[2] See Article 12 of the UDHR: *»No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.«*
[3] International Covenant on Civil and Political Rights: Uradni list RS, št. 35/92 – MP, št. 9/92.
[4] See Article 17 of the ICCPR: *»1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.«*
[5] European Convention on Human Rights: Uradni list RS, št. 33/94.
[6] See Article 8 of the ECHR: *»1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.«*
[7] Charter of Fundamental Rights of the European Union: *OJ C 326, 26.10.2012, p. 391–407.*
[8] See Article 7 of the CFREU (respect for private and family life): »*Everyone has the right to respect for his or her private and family life, home and communications.«*
[9] Constitution of the Republic of Slovenia (Slovene *Ustava Republike Slovenije):* Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121, 140, 143, 47/13 – UZ148, 47/13 – UZ90, 97, 99, 75/16 – UZ70a, 92/21 – UZ62a.
[10] See Article 35 of the CRS (Protection of the rights to privacy and personality rights): *»The inviolability of the physical and mental integrity of every person and his privacy and personality rights shall be guaranteed.«*
[11] Convention on the Rights of the Child (CRC): Uradni list RS – MP, št. 9/92.

home, or correspondence, as well as the right to protection of their honor and reputation. Finally, Article 16 of the CRC also requires State Parties to protect children from interference with or attacks on their privacy.

2 Children's Right to Privacy in the Digital Environment

The children of today are the first to be born into the digital age, and their parents are the first to be called 'digital children'.[12] Today's children leave their digital footprint from birth, some even before they are born (e.g., a parent shares a photo of a sonogram of their unborn child[13]). Parents, in such a way, shape children's digital identity/footprint through sharenting, and these disclosures can follow their children into adulthood.[14] It is, therefore, all the more important that special attention is paid to protecting children's privacy.

The digital age and digitization bring numerous advantages to our personal and professional lives. However, there are many persistent and grave risks of violating the right to privacy. With the rapid development of technologies such as social media, online tracking, and the collection of personal data, privacy protection is becoming increasingly complex. Globalisation offers many new opportunities for effective networked activities, which is the main and most distinctive aspect of the digital age.[15] Data about individuals is often collected without their informed consent or is exposed to abuse, increasing the risk of identity theft, surveillance, and manipulation. Furthermore, there are concerns about the influence that significant technology corporations have over personal data, as they often process and store data without adequate protection, leading to potential violations of individuals' privacy rights. Children are particularly vulnerable in this regard, as due to their youth and inexperience, they are often victims of privacy violations.

Children's data is collected and stored from birth onward. The collection, processing, storage, and use of personal data raise increasingly complex issues, which have also increased the intrusion into children's privacy. Smartphones, mobile data, accessibility to the internet, and other technologies have contributed to children

[12] United Nations – General Assembly, 2021, p. 13.
[13] So-called *sharenting* (*'the habitual use of social media to share children's news, images'* - Aydoğdu, Şanal Güngör & Öz, 2023).
[14] Livingstone, Stoilova & Nandagiri, 2019, p. 22.
[15] Romansky, 2022, p. 93.

spending more and more time online today. Children use smartphones for educational purposes, especially in their free time. As a result, children can access information and content almost anywhere and anytime. Additionally, activities such as watching television, communicating with peers and relatives, listening to music, and seeking commercial information have also moved online.[16]

With the expansion of the digital age, the development of information technologies, and digital networks, children's privacy has become a central issue. Children's online privacy arises in many online spaces and activities. It develops within the framework of relationships between children and public entities, interactions between children and commercial entities, and relationships between children and other individuals.[17] In their online activities, children often intentionally or unintentionally share a significant amount of personal data. Children's online data has become a valuable commodity for commercial entities, which today collect more information about children than governments.[18]

Children's privacy can be especially at risk in the home environment, in alternative forms of care, and in institutional settings, including schools and hospitals. Just like adults, children's privacy is increasingly threatened online as well. Threats to children's privacy can arise from the digital activities of others, such as peers, family members, caregivers, or strangers, from the collection and processing of data by public institutions, companies, and other organisations, as well as from criminal activities like hacking, blackmailing, identity theft, stalking, etc.[19] Children's actions can also lead to a violation of their privacy. This is particularly at risk in the digital sphere, as children, due to their young age, lack of experience, and digital skills, are often unaware of the threats and dangers that lurk in various digital activities (e.g., playing games, seeking friendships or information, or browsing the web casually). Children unwittingly and unconsciously, but often also deliberately, provide their personal data in these online activities.

[16] Smahel et al., 2020, p. 22.
[17] Blecher-Prigat, 2023, p. 260.
[18] Blecher-Prigat, 2023, p. 260.
[19] Livingstone, Stoilova & Nandagiri, 2019, p. 28.

3 Children and Data Protection

At the EU level in the field of data protection, an important step was taken in 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: GDPR) was adopted.[20] GDPR now also imposes stricter rules on how children's data can be collected and processed. Article 8 of the GDPR introduced additional obligations with the aim of ensuring a higher level of data protection for children in the context of the information society through information society services.[21] Article 8 of the GDPR provides:

> *"1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.*
>
> *Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*
>
> *2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.*
>
> *3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child."*

Article 8 of the GDPR, therefore, applies only if the processing of data a) relies on consent as a legal basis and b) if the Internet society service is being offered directly to a child.

Under the GDPR, the default age at which a person is no longer considered a child and can, therefore, give valid consent is 16. This was a new provision for the EU and brought many challenges. On the other hand, it has been in place in the US since 1998, when the Children's Online Privacy Protection Act (hereinafter: COPPA) was

[20] 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) (hereinafter: GDPR): *OJ L. 119, 4.5.2016, p. 1–88.*
[21] EDPB, 2020, p. 25.

passed. COPPA brought detailed rules for controllers collecting children's personal data.

The GDPR sets a uniform age limit of 16 years[22], after which all children can be considered to be able to consent to the processing of their personal data. The age of 16 thus constitutes a *prima facie* threshold for independent decision-making of children.[23] However, the 16-year age limit under GDPR is not absolute. An exception is made because the GDPR allows Member States to set a lower age in their national law, which may not be lower than 13 years.

Regarding the age limitation of valid consent, the GDPR so provides flexibility.[24] Thus, it can be concluded that, as already mentioned, 16 years old is set as the age defined by the GDPR for children to provide consent without parental permission. On the other hand, a range between 13 and 15 years old is provided, allowing member states to set a lower age. Thus, the age limits vary and are:

a) 13 years: Belgium, Denmark, Estonia, Finland, Latvia, Malta, Portugal, Sweden;
b) 14 years: Austria, Bulgaria, Italy, Lithuania, Spain, Cyprus;
c) 15 years: Czech Republic, France, Greece, Slovenia[25];
d) 16 years: Croatia, Germany, Hungary, Ireland, Luxembourg, Poland, Romania, Slovakia, Netherlands.[26]

[22] Regarding the age limit of 16, which allows children autonomy under the GDPR, there are also criticisms. Critics base their arguments on the fact that setting the age limit at 16 constitutes a violation of children's rights under the UNCRC. The UNCRC guarantees children the right to access information, to express their views and to participate in the decision-making processes, the right to learn and to develop, etc. Article 8(1) of the GDPR in its effect bans children younger than 16 years to actively participate in many activities on the Internet, most of which are worthy means of communication and participation, although they bear some data protection risks (Krivokapić & Adamović, 2016, p. 209 – 210).

[23] Taylor et al., 2017, p. 377.

[24] EDPB, 2020, p. 26; Macenaite & Kosta, 2017, p. 189.

[25] So Article 8 of the Personal Data Protection Act (Slovene *Zakon o varstvu osebnih podatkov (ZVOP-2):* Uradni list RS, št. 163/22): "*1) A child's consent for the use of information society services offered directly to children or for services that can reasonably be assumed to be used by children is valid if the child is 15 years old or older. If the child is younger than 15, the consent is only valid if given or approved by one of the child's parents, their guardian, or a person with parental responsibility. When the information society service is provided free of charge, consent can also be given by the child's foster parent or the representative of the institution where the child is placed. In cases where the terms of service of the information society provider prescribe a higher age for the use of these services, the age specified in the provider's terms of service shall apply. 2) The child's consent from the previous paragraph must not be conditioned by excessive terms imposed by the controller, so that the child is required to provide more personal data than is necessary for the purpose of providing such a service."*

[26] Caglar, 2021; Schofield, 2024.

In principle, age verification should not lead to excessive data processing. In other words, in some low-risk cases, it may be appropriate to simply require a new subscriber to disclose their year of birth or to fill in a form stating that they are (not) minors. However, if the processing involves a higher risk or if doubts arise as to the veracity of the user's statement, the controller should review their age verification mechanisms and consider introducing alternative verifications.[27]

To obtain 'informed consent' from a child, the controller must explain in language that is clear and plain for children how it intends to process the data it collects. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility[28] over the child. In such a case, it is the parent that is supposed to consent, then a set of information may be required that allows adults to make an informed decision.[29] The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

The GDPR parental consent requirement is a flexible standard of liability. To comply, it's enough to make reasonable attempts to obtain verifiable parental consent, rather than needing to obtain it in all cases.[30]

Thus, controllers must identify the legal age of consent in the jurisdictions in which they operate by taking into account their target demographic. In particular, it should be noted that

[27] EDPB, 2020, p. 26 and 28.
[28] Parental responsibility should be aligned with the family law. In Slovenia, parental responsibility (Slovene *starševska skrb)* is defined by Family Code (Uradni list RS, št. 15/17, 21/18 – ZNOrg, 22/19, 67/19 – ZMatR-C, 200/20 – ZOOMTVI, 94/22 – odl. US, 94/22 – odl. US, 5/23, 34/24 – odl. US) in Article 6: *1) Parental responsibility shall be the entirety of obligations and rights of parents to create, in accordance with their capacities, conditions for the comprehensive development of a child. 2) Parental responsibility shall pertain jointly to both parents.«* Article 136 of the FC provides a further definition of the content of parental responsibility: *»1) Parental responsibility shall be the obligations and rights of parents concerning care for the child's life and health, upbringing, care and treatment, supervision of the child and providing for the child's education, as well as the obligations and rights of parents concerning representation and maintenance of the child and managing the child's property. 2) Parental responsibility may be restricted to or withdrawn from one or both parents by the competent authority subject to the conditions laid down in this Code.«*
[29] EDPB, 2020, p. 26.
[30] Macenaite & Kosta, 2017, p. 177.

> "*a controller providing a cross-border service cannot always rely on complying with only the law of the Member State in which it has its main establishment but may need to comply with the respective national laws of each Member State in which it offers the information society service(s).*"

According to Recital 38 of the GDPR, children benefit from specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of children's personal data for marketing purposes or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to children. As such, Article 8 GDPR stipulates additional requirements for consent by children.

In principle, age verification should not lead to excessive data processing. In other words, in some low-risk cases, it may be appropriate to simply require a new subscriber to disclose their year of birth or to fill in a form stating that they are (not) minors. However, if the processing involves a higher risk or if doubts arise as to the veracity of the user's statement, the controller should review their age verification mechanisms and consider introducing alternative verifications.[31]

The principle of transparency requires that any information addressed to the public or the data subject be concise, easily accessible, and easy to understand and that clear and plain language and, additionally, where appropriate, visualisation be used. Given that children merit specific protection, any information and communication where processing is addressed to a child should be in such a clear and plain language that the child can easily understand.[32] Transparency will, therefore, help them to make informed decisions about what personal data they wish to share.[33]

The GDPR explicitly emphasizes that activities addressed specifically to children shall receive specific attention. As children are a particularly vulnerable group, it is important to promote public awareness and understanding of the risks, rules, safeguards, and rights in relation to processing (Article 57(1)(b) of the GDPR).

[31] EDPB, 2020, p. 26.
[32] GDPR, recital 58.
[33] ICO, 2018, p. 12; Taylor et al., 2017, p. 383.

When children reach the age of digital consent, based on their autonomy to consent to the processing of their personal data, they will have the possibility to modify or withdraw the consent given by the holder of the parental responsibility for the processing of personal data given prior to their age of digital consent (Article 7(3) of the GDPR). In accordance with the principles of fairness and accountability, the controller must inform the child about this possibility.[34]

4 Mental Health Apps' Privacy Violations

The world has gone global, and because of it, the exchange of goods and services are moving from one continent to another, causing differently regulated legal systems and their provisions to clash. One of these examples is definitely connected to the issue of digital health apps and the processing of data within them. The latter influences children's lives on a daily basis – sometimes in a positive and sometimes in a negative way. Therefore, the second part of the article will highlight the grey area of the protection of personal health data in cases of health apps, particularly in the US regulatory system, and, in this sense, the position of children. The focus on US regulations is projected because of the very intriguing regulations of this field and because of their relevance to other countries and continents. Notably, in Europe as well as everywhere else in the world, we tend to use many US apps from US providers that apply privacy policies in accordance with their law.

Interestingly, the digital mental health apps market has been growing rapidly, and by 2030, it is predicted to be worth 17.5 billion dollars.[35] Although in the US, Children's digital data in particular is protected by the Children's Online Privacy Protection Act (hereinafter: COPPA)[36], its enforcement has so far been limited to large platforms (e.g., TikTok, YouTube) and not to all other actors on the market.[37] In addition, since COPPA is an extension of the American Privacy Rights Act, it cannot be assessed in any other way but in the sense of consumer protection and its aspects.

However, the consumer's aspect is not the only relevant aspect. It must be considered that some apps do not process "just" personal data, but also personal health data, which is a sensitive group of data that should be more strongly

[34] EDPB, 2020, p. 32.
[35] Cox, 2024.
[36] S.2326 - 105th Congress (1997-1998): Children's Online Privacy Protection Act of 1998. (1998, October 1).
[37] Mostafavi, 2020.

protected. In the EU, health data and other sensitive groups of data are protected by the provisions of GDPR that generally and wholly protect the field of data protection. In contrast, in the US, the regulation of this field is relatively fragmented, and data protection is therefore distributed among various acts covering different legal fields.[38] In particular, the protection of personal health data is mainly governed by the Health Insurance Portability and Accountability Act (hereinafter: HIPAA).[39] The issue is that HIPAA does not put its focus only on health data, but also on other healthcare aspects, for instance, on insurance, the prevention of healthcare fraud and abuse, guidelines for pre-tax medical spending accounts, etc., which may, on the sidelines, cause the lack of detail in some of the norms.

Regarding HIPAA's data protection, it protects only communication between a doctor and a patient, not also sessions with some kind of specialists without a license, or, in other words, with professionals who are not "real doctors".[40] Notably, many health or medical apps offer counselling, but not necessarily by professionals with a license or the required certificate. So, at this point, it is fair to lay down a question determining with which act these (health) data are exchanged between the "so-called specialist" and the app user on a certain app, regulated and protected by? This may be a small crack in the legislation, yet an important loophole in today's digitally oriented society. When the individual behind the screen is actually a child, such a loophole opens the door to even more dangers and possible damages.

Admittedly, when it comes to questions like the one referred to, besides the national and international regulations, the company's privacy policies and other types of typical contracts take a significant role. Unfortunately, people are often unaware of their importance and do not care about their content. When it comes to minors, children or teenagers, they give it even less time and consideration. Usually, users – even from the EU territory – automatically provide their explicit consent to the app's privacy policies (which are, in cases of US app providers, made in accordance with the US regulations), so they can simply and without any trouble enter into an app and start using it.[41] While the GDPR provides stricter rules and implements the actual protection of including personal health data, it does not really matter if the

[38] Turnšek & Kraljić, 2024.
[39] HIPAA Administrative Simplification Regulation Text 45 CFR Parts 160, 162 and 164 (Unofficial version, as amended through March 26, 2013).
[40] Cox, 2024.
[41] Turnšek & Kraljić, 2024.

user consents to the use of the privacy policy of an app, which then points to US regulations.[42] This means that GDPR cannot apply in cases where explicit consent is given to other regulations. Consequently, the EU citizens cannot enjoy the rights and higher protection that is otherwise provided to them by the GDPR – their actions are then subject to the rules predicted under the typical contracts and regulations that are appointed by those.

5 Topical Cases

To provide a wholesome argumentation of the written, the article shall further on examine two cases of mental health apps, BetterHelp and Teenspace, and their privacy violations against children that were already brought to the attention of the media and authorities.

Firstly, Betterhelp is an app that offers mental health consultations to different social groups, including lgbtq+, various religious groups and also teenagers, but with a precondition of parental consent.[43] Secondly, Teenspace is a product of cooperation between the more significant mental health app Talkspace and the New York City Department of Health and Mental Hygiene. The latter was created in November 2023 with the purpose of enabling free online therapy and counselling for New York teenagers.[44] At first sight, both apps may seem as picture-perfect; however, that was not how the circumstances unfolded.

5.1 BetterHelp Case

In the case of BetterHelp, the app promised its users it would keep their data private many times – during the registration process as well as later when using the app.[45] That being said, its users had reasonable expectations that the app would actually do so. However, BetterHelp did not follow its promise, and it disclosed many of the confidential data to more prominent social platforms, including Facebook and Snapchat, all for advertising purposes.[46] What is more, BetterHelp shared that data

[42] Ibid.
[43] Federal Trade Commission, 2023.
[44] Merod, 2024.
[45] The app promised to its users to keep their data private through statements like: "Rest assured – any information provided in this questionnaire will stay private between you and your counselor." (see the the Federal Trade Commission's report).
[46] Federal Trade Commission, 2024.

with third-party advertising platforms to capitalize on these consumers' health information. On top of that, it often permitted these companies to use the information for their own research and product development.[47] The disclosed data included email addresses, IP addresses, and, more importantly, even answer given to very sensitive questions regarding their mental health status (e.g. if they are "experiencing overwhelming sadness, grief, or depression," if they're having thoughts they "would be better off dead or hurting in some way," etc.)[48].[49] While certain questions of the questionnaire were followed with false disclaimers, stating their health information would stay private between the user and their counsellor, the users were falsely deceived and manipulated by the app. Truthfully, these are the questions that some adults would not always choose to share with their friends and maybe not even with their family members. Hence, when it comes to a group of teenagers that is already hurting in some way and is in that phase in life where they are searching for their purpose and place in society, they often remain quiet and do not proceed to share such thoughts with anyone, let alone with major social media platforms. The reflection of such business was not only in the shape of legal violations or the company's monetary benefits, but also for their users, it was more about the manipulation, betrayal, and psychological damage. With that, users' rights to dignity, privacy, and data protection, not to mention the rights of many minors, were violated.[50]

Another issue arising from this case is the fact that the app demanded that teenagers fill out these questionnaires before asking for parental consent.[51] Admittedly, it cannot be expected that teenagers will pay attention or even understand the meaning of the missing legal safeguards. Nor is it realistic to expect them to foresee the possible consequences that may arise from sharing such sensitive data. In this case, the data shared were not sensitive only because of their health nature, but also because they were teenagers' data, data of a disadvantaged group of people unaware of the possible dangers. By stripping away the precondition of parental consent, the app disabled the likelihood of a minor having adult supervision. The purpose of

[47] FTC v. BetterHelp, inc. corporation, Compile, inc. and others. Case no. C-4796 - a complaint (2023, July 7), p. 2.
[48] Federal Trade Commission, 2023.
[49] FTC v. BetterHelp, inc. corporation, Compile, inc. and others. Case no. C-4796 - a complaint (2023, July 7), pp. 5-6.
[50] Turnšek & Kraljić, 2024.
[51] FTC v. BetterHelp, inc. corporation, Compile, inc. and others. Case no. C-4796 - a complaint (2023, July 7), pp. 4-5.

adult supervision and parental consent is specifically to create a possibility for adults to prevent such situations from happening. A parent (or a guardian) may notice the missing safeguards or disagree with the sharing of such sensitive data with this particular platform.

By sharing such intimate information of its users with the mentioned platforms, BetterHelp gained 30.000 – 40.000 users per every three months, which makes it 120.000 – 160.000 new users per year. Of course, inside lines that resulted in enormous profits for the app[52], as well as in huge human rights and children's rights violations for users. The latter may indicate that the app provider's interests were not entirely about helping the socially disadvantaged groups of people. It seems more likely that the leading interest was in making profits and expanding the business.

In the end, BetterHelp was charged by the Federal Trade Commission (particularly on the basis of Section 5 of the FTC Act[53], 15 U.S.C. § 45(a)) to pay 7.8 million dollars. Even though it may seem like a high amount of money at first sight, BetterHelp made incomparably more by making those privacy violations. In the year 2020, the company made over $345 million in revenue, and a year later, in 2021, they made over $720 million in revenue.[54] Arguably, the latter may question the efficiency of the sanctions imposed.

5.2 Teenspace App

Unfortunately, BetterHelp is not the only app, which violated or violates the privacy of its users. Another mental health app that made comparable violations is Teenspace. Regarding its privacy, Talkspace, as a provider of Teenspace, had some similar red flags. For example, its former employees argued that Talkspace did routine, yet unsubstantiated, examination of anonymized conversations between therapists and their clients with the purpose of extracting certain parts for marketing purposes.[55]

[52] FTC v. BetterHelp, inc. corporation, Compile, inc. and others. Case no. C-4796 - a complaint (2023, July 7), p. 4.
[53] Federal Trade Comission's Act. 15 USC Chapter , Subchapter I: Federal Trade Commission, n.d..
[54] FTC v. BetterHelp, inc. corporation, Compile, inc and others. Case no. C-4796 - a complaint (2023, July 7), p. 3.
[55] Kaur, 2024.

Teenspace was created later in 2023 and supposedly only for the teenagers' good sake. While the conversations between therapists and users were set to be protected by HIPAA, the data provided to this platform during the phase of registration did not share the enjoyment of its protection. Intriguingly, all users had to first go through a registration process, requiring quite many data (e.g., name, school, mental health history, gender identity),[56] among which not all should be classified as necessary just for registering. In fact, in the EU, that alone would constitute a breach of the "data protection principles" of data minimisation and/or purpose limitation, generally provided by the GDPR.

Additionally, the data provided during the registration process was not only left without the adequate protection of HIPAA (even though they did include personal health data), but also – teenagers gave these data without parental consent. The latter was required after the registration, not giving parents as responsible persons for their children the chance to review the privacy policies of the app prior to its usage.[57] The Teenspace app's improper use of parental consent is very similar to that of BetterHelp's. This research does not include enough cases to find a solidly established pattern of similar app providers making comparable violations. However, these two cases are certainly not the only ones to have such an unlawful model that runs against fair business practices.

Moreover, through an online "privacy-investigating" website[58] Parent Coalition for Student Privacy, discovered that when a student visits Teenspace's website, their personal data is shared with 15 ad trackers and 34 cookies, including big corporations such as Amazon, Facebook, Google, and Microsoft.[59] Admittedly, Teenspace targeted specifically teenagers, minors, and their personal health data and disclosed them to more significant platforms, even though the data disclosed presents one of the most sensitive groups of personal (health) data. Not only did Teenspace fail to provide sufficient protection for it, the app alone decided to actively make a breach and provide that data to numerous platforms. Given the city's Health Department's objective was to provide mental health counselling for minors free of charge, so

[56] Elsen-Rooney, 2024.
[57] Elsen-Rooney, 2024.
[58] An online "privacy-investigating" website they used was a so-called »Blacklight privacy tool«, which is a platform made by nonprofit newsroom, where anyone can examine any website and see if it holds any third-party's cookies, trackers, google analytics, Facebook pixel etc. (for more see: https://themarkup.org/blacklight).
[59] Admin, 2024.

anyone could afford it and benefit from it, such intentional data breaches may contest the true purpose of this 26 million dollars' worth partnership between the app and the city and suggest their agenda had some other aims or motives. Admittedly, the similarities between the two apps were not only in their ways of violating their users' privacy rights, but also in having the US Senators question their practices.[60] The latter, however, was not a sufficient tool for stopping Talkspace or BetterHelp from committing the alleged violations. That was approximately two years before the Federal Trade Commission took steps against the BetterHelp app, as well as two years before the proceeding against Talkspace.

Finally, a class action was filed against Talkspace for sharing an extensive scope of personal data (including personal mental health data even) of minors with TikTok,[61] which raised an alarm regarding the services of Teenspace in general.[62] A plaintiff was allegedly supported by thousands of Talkspace users whose rights were violated.[63] When this class action arose in August 2024, the extension of Talkspace – Teenspace's services and regulations was also starting to raise some concerns. Consequently, the Coalition for Student Privacy, New York Civil Liberties Union, and AI for Families all together expressed concerns to the New York City's Mayor, Health Commissioner, and the Deputy Mayor for Health and Human Services.[64] Although the matter is still ongoing, it may get a similar ending as BetterHelp's case.

6 Suggestions For More Effective Sanctions

Based on the examined topics and cases of BetterHelp and Talkspace/Teenspace, the larger platforms do not provide sufficient privacy policies nor respect for human rights and children's rights. At first, both apps were handled with a "softer remedy" (questioning by the senators) and then, one was served with financial sanctions and the other recently received a class action, which remains unsolved.

Considering BetterHelp's case, which was already concluded, the app made a settlement for far less money than it gained by making those violations. In other words, by doing those privacy violations and being charged, BetterHelp still stayed

[60] Warren, 2022.
[61] Rizzi, 2024.
[62] Rizzi, 2024.
[63] Courtney Mitchener v. Talkspace Network llc., US District Court Of California, Case 2:24-cv-07067, p. 6, para 23.
[64] Courtney Mitchener v. Talkspace Network llc., US District Court Of California, Case 2:24-cv-07067, p. 6, para 23.

in a few hundred million dollars in profit. The latter makes the sanction ineffective. Admittedly, the people whose rights were violated are entitled to certain refunds from the sanction imposed, which shall represent satisfaction for them. However, such a sanction cannot be understood as a deterrence measure for the misconduct. Deterrence measures should lead with the purpose of reforming the subject and his actions, but that did not happen in the present case. Admittedly, BetterHelp has improved and broadened its privacy policies, yet it has not stopped collaborating with third-party advertising platforms and earning money from disclosing users' data.

Considering the digital mental health apps market is in its rapidly developing era, it is of no surprise the companies' net worth is rising to unimaginable amounts. Therefore, when it comes to sanctioning, talking numbers in the light of financial punishment makes no sense. The most important element of their business are users – whether that means adults, children, teenagers or young adults – as they are the ones providing the very scalable data and direct payments to the app by paying additional packages or services. Therefore, the most efficient sanction for such violations and apps would not be monetary but to freeze their business until the correction of their unlawful business practice.

When it comes to the flooded market of mental health apps, users are used to use one app in particular, but if the one does not work for a while, they will quickly and easily find another comparable one. It is unlikely that the user, who seeks such services and opens an account at another app, will actually come back to the previous app, when they have already gotten comfortable with that newly chosen one. This way, the "frozen" app would start losing its users, but only until the privacy policies and the rightful respect for the privacy of its users were corrected. Then, the authority could unfreeze their app and enable its return to their normal business. If the app does not correct its policies and services in a reasonable time, that could lead to the loss of numerous users and, consequently, to high amounts of lost profit. The app provider would therefore be motivated to change his wrongdoing.

While a provider of a particular app might not feel deterred when he gets the obligation to cover a relatively low financial sanction (taking into account that it already gained more than it would without sharing users' data for advertising purposes), its attitude should be turning if it came to freezing their business and for

that limited time stop gaining new users, losing present users together with a loss of profit, daily revenue and more. Such an approach would cause apps to lose lots of money in the long run. In comparison, paying a one-time amount estimated at around a few million or approximately ten million dollars, when they are already making hundreds of millions of dollars, represents no deterrence and definitely no motivation to change.

In consideration of this, by implementing such sanctions, the state would not be imposing a specific number, as it is mainly seen in regulations, which could stir the opinions and raise doubts of the public. Nonetheless, the sanctions imposed are most of the times too low and, because of it, ineffective, not realizing their fundamental purpose – to deter and to reform the subject of misconduct.

Another solution to improve the effectiveness of the sanctions to some degree would be to propose them in the sense of a percentage of the annual turnover or revenue of the preceding financial year. For instance, this approach was already taken by the GDPR, which gives an option for the company to be served with a sanction leading up to the amount of 10 million euros or at the amount of two percent of the company's annual turnover of the preceding financial year – whichever is higher. With such an approach, the regulations are not imposing sanctions in a relatively small setting of the financial amount (e.g., from x dollars to y dollars), but allow the Tech Giants to be punished with higher sanctions and smaller players with smaller ones. Meaning, the smaller companies would be punished in accordance with their financial capacity, not to make them bankrupt, but still high enough to make them regret making the violations. However, in my opinion, the most prominent actors that turn billions of dollars yearly are still not getting the proper sanctions under the GDPR's approach. That is the reason why we believe this solution should improve the effectiveness of the sanctions to some degree.

Therefore, if we want to stop large platforms from making violations, the sanctions must change. Otherwise, the functioning of various apps will remain concentrated on making the most profits possible, the same violations will continue happening, and sanctions will be paid off repeatedly. That is why the decision-makers should first establish the purpose and the aim of the sanction and then consider about the most adequate steps to get there.

7 Conclusion

As personal data is becoming a new currency, the field is getting more valued and, with that, better protected. Even though the personal health data collected by or shared with an app (whether it is a medical app, fitness, or mental health app) during the registration process falls into the scope of a so-called grey area – not covered by the HIPAA – it does not mean this data is not protected at all. The example of BetterHelp shows that there are certain "watchdogs" besides the court who sense such privacy violations and impose sanctions, trying to prevent the continuance of such infringements. Furthermore, from the case of Talkspace, it can be learned that such app provider who is violating its users' privacy can be served with a class action lawsuit. Even though the cases of neither Teenspace nor Talkspace are not yet closed, by now the media has spread the news, as well as warnings about the privacy violations. In addition, we can see the US has recognised the importance of children's personal (health) data protection by the proposed amendments for the American Privacy Rights Act 2024 and Children's Online Privacy Protection Act.

Last but not least, data protection breaches are becoming a serious threat to our privacy and with that also to our rights in general. However, to have an actual breach, we must first have a provision in a legal act or code that is being violated. Since law always follows the footsteps of society, it is time that legal acts (or decision-makers) start to consider the technological development and innovations that come with it and regulate it accordingly. When it comes to disadvantaged groups of people, especially children that cannot really protect themselves by themselves, it is of significant importance that law does that for them.

References

Admin. (2024) 'Privacy concerns with NYC student use of Teenspace online counseling service'. *Parent Coalition for Student Privacy, 2024, September 10*. Retrieved from: https://studentprivacymatters.org/privacy-concerns-about-nycs-promotion-of-the-teenspace-online-counseling-service/ (accessed: 29 October 2024).

Aydoğdu, F., Şanal Güngör, B. & Öz, T. A. (2023) 'Does sharing bring happiness? Understanding the sharenting phenomenon'. *Children and Youth Services Review*, 154, p. 107122.

Blecher-Prigat, A. (2023) 'Lost Between Data and Family? Shortcomings of Current Understandings of the Law'. In: Dethloff, N., Kaesling, K., Specht-Riemenschneider, L. (eds) *Families and New Media. Juridicum – Schriften zum Medien-, Informations- und Datenrecht*, pp. 259-272. Wiesbaden: Springer. https://doi.org/10.1007/978-3-658-39664-0_12

Caglar, C. (2021) 'Children's Right to Privacy and Data Protection: Does the Article on Conditions Applicable to Child's Consent Under the GDPR Tackle the Challenges of the Digital Era or Create Further Confusion?'. *European Journal of Law and Technology*, 12(2). Retrieved from: https://ejlt.org/index.php/ejlt/article/view/828/1025 (accessed: 2 January 2025).

Charter of Fundamental Rights of the European Union: *OJ C 326, 26.10.2012, p. 391–407.*

Constitution of the Republic of Slovenia (Slovene *Ustava Republike Slovenije):* Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121, 140, 143, 47/13 – UZ148, 47/13 – UZ90, 97, 99, 75/16 – UZ70a, 92/21 – UZ62a.

Convention on the Rights of the Child (CRC): Uradni list RS – MP, št. 9/92.

Courtney Mitchener v. Talkspace Network llc., US District Court Of California, Case 2:24-cv-07067. Retrieved from: https://www.classaction.org/media/mitchener-v-talkspace-network-llc.pdf (accessed: 28 October 2024).

Cox, D. (2024) 'They thought they were doing good but it made people worse: why mental health apps are under scrutiny'. *The Guardian*, 2024, February 4. Retrieved from: https://www.theguardian.com/society/2024/feb/04/they-thought-they-were-doing-good-but-it-made-people-worse-why-mental-health-apps-are-under-scrutiny (accessed: 25 October 2024).

Elsen-Rooney, M. (2024, September 10) 'Data privacy advocates raise alarm over NYC's free teen teletherapy program'. *Chalkbeat*, 2024, September 10. Retrieved from: https://www.chalkbeat.org/newyork/2024/09/10/privacy-advocates-raise-concerns-free-teletherapy-teens-data/ (accessed: 29 October 2024).

European Convention on Human Rights: Uradni list RS, št. 33/94.

European Data Protection Board (EDPB) (2020) 'Guidelines 05/2020 on consent under Regulation 2016/679', Version 1.1 Adopted on 4 May 2020. Retrieved from: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (accessed: 3 January 2025).

Family Code (Slovene *Družinski zakonik):* Uradni list RS, št. 15/17, 21/18 – ZNOrg, 22/19, 67/19 – ZMatR-C, 200/20 – ZOOMTVI, 94/22 – odl. US, 94/22 – odl. US, 5/23, 34/24 – odl. US.

Federal Trade Comission's Act. 15 USC chapter 2, subchapter I: Federal Trade Commission. (n.d.). Retrived from: https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter2-subchapter1&edition=prelim (accessed: 28 October 2024).

Federal Trade Commission (2024) BetterHelp Refunds, 2024, November 12. Retrieved from: https://www.ftc.gov/enforcement/refunds/betterhelp-refunds (accessed: 28 October 2024).

Federal Trade Commission. (2023) FTC says online counseling service BetterHelp pushed people into handing over health information – and broke its privacy promises, 2023, October 5. Retrieved from: https://www.ftc.gov/business-guidance/blog/2023/03/ftc-says-online-counseling-service-betterhelp-pushed-people-handing-over-health-information-broke (accessed: 28 October 2024).

FTC v. BetterHelp, inc. corporation, Compile, inc and others. Complaint in a case no. C-4796 (2023, July 7).

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

ICO (2018) 'Applications – Children and the GDPR'. Retrived from: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf (accessed: 1 January 2025).

International Covenant on Civil and Political Rights: Uradni list RS, št. 35/92 – MP, št. 9/92.

Kaur, R. (2024b, November 2) 'TalkSpace controversy: EXAMINED [2024]'. *Therapy Helpers.* Retrieved from: https://therapyhelpers.com/blog/talkspace-controversy/ (accessed: 29 October 2024).

Krivokapić, D. & Adamović, J. (2016) 'Impact of General Data Protection Regulation on Children's Rights in Digital Environment', *Annals FLB – Belgrade Law Review*, 64(3), pp. 205-220.

Livingstone, S., Stoilova, M. & Nandagiri, R. (2019) *Children's data and privacy online: Growing up in a digital age. An evidence review*. London: London School of Economics and Political Science.

Macenaite, M. & Kosta, E. (2017) 'Consent for processing children's personal data in the EU: following in US footsteps?', *Information & Communications Technology Law*, 26(2), pp. 146–197. doi: 10.1080/13600834.2017.1321096.

Merod, A. (2024) '$26M Talkspace contract with NYC stirs student data privacy concerns'. *K-12 Dive*. 2024, September 16. Retrieved from: https://www.k12dive.com/news/talkspace-nyc-data-privacy-teenspace/727070/ (accessed: 28 October 2024).

Mostafavi, B. (2020) 'Some Children at Higher Risk of Privacy Violations from Digital Apps'. *Michigan Medicine – University of Michigan* (2020, September 8). Retrieved from: https://www.michiganmedicine.org/health-lab/some-children-higher-risk-privacy-violations-digital-apps. (accessed: 3 January 2025).

Personal Data Protection Act (Slovene *Zakon o varstvu osebnih podatkov (ZVOP-2)):* Uradni list RS, št. 163/22, 40/25 – ZInfV-1.

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*.

Rizzi, C. (2024, August 30) 'Talkspace Lawsuit Claims Therapy Website Secretly Shares User Data with TikTok'. *ClassAction.org*. Retrieved from: https://www.classaction.org/news/talkspace-lawsuit-claims-therapy-website-secretly-shares-user-data-with-tiktok (accessed: 3 January 2025).

Romansky, R. (2022) 'Digital Age and Personal Data Protection'. *International Journal on Information Technologies & Security*, 14(3), pp. 89-100.

S.2326 - 105th Congress (1997-1998): Children's Online Privacy Protection Act of 1998. (1998, October 1). Retrieved from: https://www.congress.gov/bill/105th-congress/senate-bill/2326 (accessed: 29 October 2024).

Schofield, M. (2024) '*GDPR Age of Consent Inst't Child's Play'*. Retrieved from: https://www.skillcast.com/blog/gdpr-age-consent-not-childs-play (accessed: 2 January 2025).

Taylor, M. J., Dove, E. S., Laurie, G., & Townend, D. (2018) 'When can the Child Speak for Herself? The Limits of Parental Consent in Data Protection Law for Health Research', *Medical law review*, 26(3), pp. 369–391. https://doi.org/10.1093/medlaw/fwx052

Turnšek, E. & Kraljić, S. (2024) 'The Protection of Sensitive Personal Data and Privacy in the US and EU with a Focus on Health Data circulating through Health Apps', *Balkan Social Science Review*, 24, pp. 179-205. https://doi.org/10.46763/BSSR242424179t

United Nations – General Assembly (2021) '*Artificial intelligence and privacy, and children's privacy - Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci*', A/HRC/46/37, 25 January 2021. Retrieved from: https://www.ohchr.org/en/documents/thematic-reports/ahrc4637-artificial-intelligence-and-privacy-and-childrens-privacy (accessed: 3 January 2025).

Universal Declaration of Human Rights: Uradni list RS, št. 24/18.

Warren, E. (2022) 'Warren, Booker, Wyden Call on Mental Health Apps to Provide Answers on Data Privacy and Sharing Practices that May Put Patients' Data at Risk of Exploitation'. (2022, June 23). Retrieved from: https://www.warren.senate.gov/oversight/letters/warren-booker-wyden-call-on-mental-health-apps-to-provide-answers-on-data-privacy-and-sharing-practices-that-may-put-patients-data-at-risk-of-exploitation (accessed: 29 October 2024).