TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Olga Vovk 177316YVEM

PRIVACY AND SECURITY EVALUATION OF MENTAL HEALTH MOBILE APPLICATIONS

Master's thesis

Supervisor: Priit Kruus
MSc

Co-supervisor: Matteo Cagnazzo
MSc

Tallinn 2019

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Olga Vovk 177316YVEM

VAIMSE TERVISE MOBIILIRAKENDUSTE PRIVAATSUSE JA TURVALISUSE ANALÜÜS

Magistritöö

Juhendaja: Priit Kruus
Magistrikraad
Juhendaja: Matteo Cagnazzo
Magistrikraad

Tallinn 2019

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Olga Vovk

18.05.2019

Abstract

Skyrocketing development of information and communication technologies introduced a wide range of new opportunities in different areas of expertise. Health care is not an exception: today, in the 21st century, it becomes more and more digitalized through the use of mobile technologies. As a result, millions of people all over the world become users of mobile health applications, including those tackling mental health. Despite the benefits coming along with managing mental health through mobile applications, the latter may be harmful as well - due to the lack of supervision, mental health applications may have significant risks to users' privacy and security. Thereby, the aim to be achieved with this master thesis was to perform a comprehensive analysis of top-rated mental health mobile applications in terms of privacy and security.

Relevant academic literature was studied to examine current situation through the research about mental health mobile applications privacy and security. Moreover, the EU and the US legislation regarding mobile applications was studied; requirements were compared. In order to conduct this study, several research methods were used. Firstly, mobile applications (N=20) were downloaded, and legal aspects of their privacy policies were analyzed using two assessment frameworks, American Psychiatric Association (APA) App Evaluation Model and European General Data Protection Regulation (GDPR) requirements. Secondly, implementation of legal requirements and statement from privacy policy into practice were checked using applications installed on the device. Finally, in order to make in-depth analysis from a technical perspective and reveal security-related and data sharing information, static code analysis was performed.

Findings of the study reveal that the majority of applications violate at least one or more privacy and security requirements. Furthermore, only 10 (50%) of evaluated applications can be considered as acceptable based on the APA App Evaluation Model and only 4 (20%) meet GDPR requirements.

This thesis is written in English and is 60 pages long, including 6 chapters, 12 figures and 2 tables.

Annotatsioon

Vaimse tervise mobilirakenduste privaatsuse ja turvalisuse analüüs

Info- ja kommunikatsioonitehnoloogia kiire areng on avanud uusi tehnoloogilisi võimalusi erinevates eluvaldkondades. Tervishoid ei ole erand, kus tänu mobiilsetele tehnoloogiatele on digitaaliseeritus järk-järgult paranenud. Tänaseks kasutavad mobiilse tervise, sealhulgas vaimse rakendusi miljonid inimesed maailmas. Vaatamata vaimse tervise haldamisega kaasnevatele eelistele, võib see ka kahjulikuks osutuda – kuna nende rakenduste üle puudub järelvalve, võivad need kujutada endast märkimisväärset ohtu kasutajate privaatsusele ja turvalisusele. Seetõttu oli käesoleva magistritöö eesmärgiks viia läbi laiaulatuslik analüüs parimaks hinnatud vaimse tervise valdkonna mobiilirakenduste osas, keskendudes privaatsusele ja turvalisusele.

Hetkeolukorra väljaselgitamiseks uuriti vaimse tervise mobiilirakenduste privaatsus ja turvalisuse aspekte, lähtudes asjakohasest teaduskirjandusest. Lisaks uuriti Euroopa Liidu ja USA mobiilirakendusi puudutavat seadusandlust. Käesoleva uurimistöö läbiviimisel rakendati järgnevat metoodikat. Esmalt laaditi alla mobiilirakendused (N=20) ning hinnati nende privaatsuspoliitika õiguslikke aspekte lähtuvalt kahest hindamisraamistikust: Ameerika Psühhiaatrite Liidu (APA) Rakenduse Hindamise Mudeli ning Euroopa Isikuandmete Kaitse Üldmääruse (GDPR) alusel. Teiseks kontrolliti kuivõrd tegelikult seadmesse installeeritud rakendused neid õiguslikke nõudeid ja privaatsuspoliitikat rakendavad. Lõpuks viidi läbi koodi staatiline analüüs, koostamaks põhjalikku tehnilist analüüsi ning paljastamaks turvalisuse ja andmete jagamisega seotud asjaolusid.

Uuringu tulemused näitavad, et enamik rakendusi rikub vähemalt ühte või mitut privaatsus- ja turvalisusnõuet. Lisaks ainult ainult kümmet (so 50%) hinnatud rakendustest võib pidada aksepteeritavaks APA Mobiilirakenduste Hindamise Mudeli põhjal ning ainult neli (so 20%) vastavad GDPR-I nõuetele.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 60 leheküljel, 6 peatükki, 12 joonist, 2 tabelit.

List of abbreviations and terms

AI	Artificial Intelligence
APA	American Psychiatric Association
APK	Android Application Package
App	Application
CCPA	California Consumer Privacy Act
GDPR	General Data Protection Regulation
FDA	Food and Drug Administration
GPS	Global Positioning System
HIPPA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
MDD	Medical Devices Directive
MDR	Medical Devices Regulation
mHealth	Mobile Health
TSL	Transport Layer Security

Table of contents

List of figures

List of tables

1 Introduction

1.1 Background

Mobile technologies play an important role in our everyday life. People use mobile applications for communication, navigation, entertaining, managing lifestyle. Health care is also one of the fields on which mobile apps have a significant impact. More than 325,000 mobile health (mHealth) apps are available on the market and this number is constantly growing [1]. Mobile health applications provide an enormous variety of functions related to human health. Mobile devices can be used to measure blood pressure, heart rate, can help with self-check of vision, hearing, lungs capacity. Health apps that are intended to assist with mental health are a significant part on the app market and it is expected their number will increase [2].

According to the research, the applications can help people to manage their mental condition [3]. Mobile health applications play different roles in patients' therapy. There are different opinions about the role of mHealth in therapy. Some researchers see apps as an alternative to traditional therapy [4], while others state mobile apps are not suitable as its substitute [5]. Furthermore, apps can serve as additional supportive tool in therapist-patient interaction [6]. Mental health apps offer a wide range of services depending on the user's needs: they provide telehealth services – connect to the licensed mental health specialist. With other apps, users can keep a mood diary, food diary and activity tracking, share thoughts with other people or char with Artificial Intelligence (AI) bot [3]. Some apps use gamification to help users deal with mental conditions; others provide guidelines on how to cope with stress and anxiety by breathing exercises and meditation, or listening to calming music and sounds.

No doubts, there are benefits of using mobile apps: their prices are lower compared to traditional therapy, many apps are offered free of charge, available 24/7, anytime when the user needs at any place. mHealth apps can help overcome an emotional gap between the patient and health care provider by creating a strong patient-doctor bond [7]. Additionally, an app can be a tool for self-education about managing condition [8].

Along those benefits come significant risks – a lot of mental health mobile apps and their effectiveness may be an overestimate. The effectiveness of one or another app is not necessarily scientifically proven – lack of evidence base, as well as the possibility to provide a user with incorrect information, may lead to negative effects while using an app [9]. Moreover, mobile health apps may pose significant risks to the user's privacy and security [10], [11]. Those risks occur due to the nature of data that is processed and stored by the mHealth app. Especially high risk is posed by applications that contain sensitive and vulnerable information about users [12]. Depending on functionality mHealth apps can access to health-related and other sensitive personal data, electronic health records, prescribed medication, which may be eventually misused. Health care data is on high demand on the black market [13] and mobile apps might be an easy target to get this data. As a further matter, recent research showed that the information stored on mobile devices is on higher demand from the attacker's perspective [14]. For this reason, mental health mobile apps analysis is the way to evaluate whether apps take respective measures to ensure proper privacy and security for users' data.

1.2 Statement of problem

As of today, in the 21st century, privacy and security concerns appear to be an important topic. Recent events, such as those involving WhatsApp [15], Facebook [16], as well as health-related apps My Fitness Pal [17] and My Heritage [18], led to disclosure of unlawful data collection and sharing, and major data breaches, which include personal data of millions of mobile application users, and bring attention to the field.

Despite the fact that mental health mobile apps possess a risk related to the collection of a wide scope of sensitive data, they remain outside specific governmental regulation and due to that their privacy and security level might be very low.

Studies concerning mobile apps' privacy and security issues usually focus only on one aspect, for example, privacy policy review or data sharing disclosure.

In contrast, this research aims to perform comprehensive analysis in mental health mobile applications by including legal policy assessment, to perform analysis of actual implementation statement from the policy in the app; and to conduct static code analysis

to check whether the information in privacy policy meets the reality and to discover information not displayed in the privacy policy.

As of today, there are no extensive studies which include legal and technical aspects of mental health mobile applications. Moreover, none of the studies of mental health mobile apps privacy and security was conducted after the General Data Protection Regulation (GDPR) came into force in May 2018. Therefore, the main contributions of this master thesis are to highlight challenges in the field that need to be addressed; and to analyze whether the most top-rated applications with high numbers of downloads are private and secure. Moreover, this thesis intends to explain the difference between privacy and security requirements in the EU and the US.

This thesis is structured in 6 chapters and the content can be summarized as follows:

- Chapter 1 introduces the thesis topic, aims to be achieved, research questions and includes an overview of the current state of the research.
- Chapter 2 constitutes an overview of privacy and security regulations and guidelines in the EU and the US applicable for mobile health applications.
- Chapter 3 focuses on the methods applied in the research and explains in detail how the analysis was done and what tools were used.
- Chapter 4 presents the results of the analysis.
- Chapter 5 summarizes the key findings of the research, discusses the results, provides recommendations regarding applications' privacy and security improvement, points out the limitations and gives an outlook towards further research.
- The thesis is concluded with chapter 6 which summarizes the whole research.

1.3 Aim and research questions

The aim of this study is to analyze the top-rated mental health mobile apps in terms of privacy and security.

This study seeks to determine whether the most popular and high rated mental mHealth apps are compliant to the set standards and legal requirements.

1. Are the most popular mental health mobile apps General Data Protection Regulation (GDPR) compliant?
2. Are the most popular mental health mobile apps acceptable in terms of privacy and security from the American Psychiatric Association (APA) perspective?
3. What are the main problems with apps, that are not GDPR compliant and not APA acceptable? How those issues can be solved?
4. What are the differences in EU and US regulations regarding mental health mobile apps privacy and security?

1.4 Identifying relevant literature

In order to examine the most important and relevant studies regarding mental mobile health applications security and privacy issues, a literature overview was conducted. To find studies carried out by other researchers Google Scholar, PubMed database and Tallinn University of Technology online library were used. While searching for literature to overview in relation to this study, literature published in English between 2013-2019 was considered. The search was performed using the next keywords and their combination: “mobile apps”, “mental health apps” “privacy”, “security”, “GDPR”. The EU and US laws were accessed on the official web-pages. A literature overview performed for this research includes 65 research papers that introduce the following: problems regarding the mobile application privacy and security, mental health applications privacy and security issues, legal regulation and guidelines for mobile health apps, frameworks for mental health mobile apps assessment.

There are several articles dedicated to mental health applications and some of them include privacy and security-related questions as part of the research. The article “Mental Health Apps: Innovations, Risks and Ethical Considerations” written in 2014 mention data collection by apps as one of the major risks because of the value of private data, health care data for cybercriminals. The author also mentioned the lack of clear measures and regulations to guaranty mental health apps safety [4]. Some of the articles, as for instance “Towards a Framework for Evaluating Mobile Mental Health Apps” [19] make an attempt to build a model for mobile apps evaluation, which includes privacy and security as one on the measurements.

However, studies about health apps privacy and security are conducted as well. One of the most recent studies “Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice” published it the beginning of 2018 provides health apps evaluation from the technical point of view. This research is done for a wide scope of mobile health ones; alongside with technical assessment, GDPR readiness is evaluated as well [11]. Another article “Reviewing the data security and privacy policies of mobile apps for depression” [20] is dedicated to the app's assessment intent to evaluate apps solely based on their privacy policy. Some of the studies cover basic security and privacy issue for a wide range of mobile apps, others on the opposite use single application for the case study. For example, “Are mHealth apps secure?” is the case study about a Fitness Tracker, which includes privacy policy analysis and technical insecurities detection [21].

All of those studies have shown significant problems with mobile apps privacy and security. There are just a few studies specifically dedicated to mental health mobile applications privacy and security. Moreover, none of those studies was conducted after GDPR came into force. Potentially, the GDPR has a positive impact on increasing privacy and security level, but most likely it has not solved all existing problems.
Literature overview led to several key findings:

- Mental health apps deal with a wide range of sensitive information and due to that possess a high risk;
- The majority of mobile apps remains out of the scope of special legal regulation;
- The most comprehensive mental health mobile apps evaluation framework is provided by APA;
- There are studies that are based on mobile apps GDRP assessment, but none of them was conducted after GDPR came into force.

2 Privacy and security regulations in the EU and US

2.1 Overview of privacy and security regulations and guidelines regarding mobile health applications in the EU and US

There are numbers of studies making an attempted to define the concept of privacy and security. The concept of privacy appeared a long before the age of the Internet. In past decades academics define privacy as personhood, intimacy, secrecy and control over information [22]. In the context of information and communication technology, privacy is regarded as information privacy or data privacy. By those terms authors understand a control that person has over how and where information about him or her is acquired, stored and processed [23].

Security means the implementation of comprehensive measures to prevent unauthorized access, modification, use, share or erasure of stored or processed data, as well as to prevent denial of service and to protect the system from physical harm [24]. Information security is implemented in the practice as a mean of defence of information. There are various legal acts and regulations surrounding the issue of data privacy and security [25].

The EU General Data Protection Regulation, which came into force on 25 May 2018, becomes one of the most important privacy and security legal regulation in Europe and outside. The GDPR replaced the Data Protection Directive 1995 (Directive 95/46/EC) and aims not only increase privacy and security but to ensure them by default, meaning that data protection is kept in mind thought all activities [26]. The GDPR brought the most important and significant changes in data privacy legislation for the last 20 years. The Regulation was introduced due to several reasons: for better protection of personal data, for harmonization privacy legislation across EU member states, and to reshare organizations approach to handle personal data [27]. The GDPR provides the EU residents with greater control over their data by the right to be informed over what, how, why, where and by whom personal data is processed.

The GDPR sets out seven key principles needed to be followed by those who are processing personal data:

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimization;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality (security);
- Accountability.

Adopting the GDPR was a large step towards data protection. The Regulation applies to "personal data", which according to the article 4 of GDPR, means any information related to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly [28].

The GDPR is binding in its entirety on all EU countries. As a regulation, GDPR applies automatically and uniformly to all EU countries as soon as it enters into force, without needing to be transposed into national law [29]. The GDPR applies even beyond the borders of the EU. Any entity, that process personal data of EU residents, is obliged to be compliant with the GDPR. Furthermore, article 3 of the GDPR specified that companies outside the EU, which offer services to EU residents are also obliged to be GDPR compliant. Currently, there are no doubts about the significant impact of GDPR. It is paramount to understand how this regulation changes data protection not only for European countries but also for the whole world.

Certain categories of data receive special protection under the GDPR. The article 9 of the GDPR refers to "special categories of personal data" which include "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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" [28]. "Data concerning health" is defined in the article 4 of the GDPR as personal data "related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status", belong to the special category of data [28].

In order to be GDPR compliant, entities need to implement technical and organizational measures. According to the Regulation, the misuse of personal data leads to serious consequences to the violators. Infringements of the GDPR provisions shall be subject to fines up to 20 000 000 EUR, or up to 4 % of the total worldwide annual turnover whichever is higher [28]. This means privacy and security violations discovered in any event as, for instance, data breach or claim from the user, will make not only reputational damage to the company but may also cause serious financial consequences.

The article 5 of the GDPR introduces "data controller" and "data processor" terms as a natural or legal person, public authority or other body that process personal data from the natural person ("data subject"), but data processor does this on behalf of the data controller. The data controller is mainly responsible for personal data protection via secure data collection and processing, while the processor is responsible within the score of its activity [28].

In contrast to EU, US legislation is more decentralized. Additionally, there is no comprehensive information privacy law, it's rather sectorial [30]. The most important privacy and security regulation at the federal level in the health care field is Health Information Privacy and Portability Act (HIPAA). The HIPAA came into force in 1996, define legal frameworks for personal health information collecting and processing by health care providers in the US. The main aim this act is to safeguard patient personal health information (PHI) which is defined as the "information that relates to the past, present, or future physical or mental health or condition of an individual, which identifies the individual and that is transmitted or maintained by electronic media or in any other form or medium." [31]. It is important to notice the significant difference between the scope of law application. If GDPR is mandatory for all entities, that collect and/or process personal data, including health-related data, HIPAA regulates only privacy and security if health care provider or health care clearinghouses are involved, or if concerning the health plan [32].

Due to the fact that mobile health applications are related directly to managing human health they might be under special regulation. The head institution in the US that defines this issue via its regulation is the Food and Drug Administration (FDA). FDA defines mobile apps as software programs that run on smartphones and other mobile communication devices [33]. For mobile application to be considered as medical, it has

to meet the definition of a medical device which means " intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, [34] or intended to be used as an accessory to a regulated medical device or to transform a mobile platform into a regulated medical device [33].

According to the FDA guidance regarding mobile medical applications, many mobile apps are not considered to be medical devices, which mean they do not meet the definition of a medical device or do meet the definition but since they pose a lower risk to the public, they remain out of the scope of the FDA regulation [33]. The vast majority of mobile apps currently available on the market are not regulated by FDA. Considering FDA's hands-off approach there is little to no regulation specifically over mental health apps [35].

The most important laws within the EU in medical equipment and software regulation are Medical Devices Directive 93/42/EEC (MDD) [36] that came into force in 1993 and was substituted with Medical Devices Regulation EU 2017/745 (MDR) [37] in 2017. Transition period to Medical Devices Regulation was started May 2017 and will last till May 2020.

Both MDD and MDR regulate medical devices as well as software related to medical devices or standalone software. Under the article 1 of the MDD medical device is any device or combination of devices used for diagnostic or therapeutical purposes meaning they are intended to be used for "detecting, diagnosing, monitoring or treating physiological conditions, states of health, illnesses or congenital deformities" or "to support, modify, replace or restore biological functions or structures" [36]. According to the Directive, standalone software considered to be medical device and qualified as such. MDR use similar approach in terminology definition. The article 2 of the MDR defines medical device as device, software and their combination used with purposes of "diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease" [37].

MDR brought significant changes in medical devices regulations. Nevertheless, the regulation regarding mobile health application basically remains the same and most of the application freely available on the marker remains out of the scope of MDR. Additionally, the vast majority of those apps point out that they cannot be considered as

medical devices, and if the user seeks medical advice he or she needs to consult with the licensed professional.

Therefore, the EU issued guidelines to evaluate mHealth apps not regulated by specific legal acts. Those guidelines are not mandatory to follow, they only provide recommendations. Guidelines aim to provide assessment whether apps are: reliable, desirable, credible, safe, secure, transparent, usable, effective and stable. To evaluate whether the app is private and secure guidelines provide a list of question such as if consent is asked, which data is collected and how used, if there is encryption in place, if data is stored securely, and if other GDPR principles are followed [38].

2.2 Privacy and security requirements under GDPR and APA

Privacy policy. One of the most important concepts under the GDPR is transparency. The privacy policy provides users with information about what is data collected, how it is stored and handled, and to whom it might be shared. According to the GDPR principles, the data controller must ensure that privacy policy is easily accessible for users and provides specific information about data collection and processing [28].

The privacy policy is required if personal data from users is collected. Nevertheless, it is necessary to understand what personal data vary between EU and other countries. Overall data collected by applications might be divided into two major categories: data concerning natural person such as name, date of birth and technical data such as information about the personal device. Data concerning a natural person is undoubtedly personal data; it is defined as personal by the EU and US laws. The question whether technical data concerning the user's device is debatable and the answer depends on many factors; also, from which perspective evaluation is carried out.

As it was mentioned above, the US does not have a centralized act, for personal data protection, rather a combination of legislation, regulation, and self-regulation. This approach gives companies more freedom to implement their own policies and develop their own technology for data protection and privacy. As a general approach used by US entities is that information which does not directly link to a natural person, like device IP or cookies is not considered as personal information. For example, the privacy policy of

the American Psychiatric Association defines IP addresses and cookies as non-personal data [39].

On the opposite, the GDPR defines technical information collected from the user's device as personal data under certain conditions. According to the article 4 of the GDPR "personal data" among other identifiers includes an online identifier, which means that even application does not collect personal data such as user's name, date of birth or email; the user still needs to be informed what data is collected [28]. Furthermore, recital 30 of the GDPR states that "natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags" [28]. All application by their nature collect at least minimum technical information about user's device such as device type, Internet Protocol address (IP), operating system (OS) version. Under the GDPR this means as long as technical information is collected privacy policy is required.

As it was mentioned before, IP addresses and cookies might be considered as personal data from the GDPR perspective if they can link to direct or indirect identification of a natural person. For example, if a dynamic IP address which is changed from time to time and depends on location will be combined with information from the Internet service provider about assigning this address, a natural person can actually be identified [40]. According to the GDPR combination of identifiers linked together are also considered as personal data. Even if the mobile app does not provide an option to create an account, this app may still collect personal data. In case only technical information about the device is collected, it still might be combined with other data, for instance, GPS services provided by the app to define location. The result of this combination can cause natural person identification which means application should have a privacy policy.

Data collection. The article 5 of GDPR introduce data minimization principle according to which collected personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". In other words, personal data that is not related to provided service shall not be collected [28]. There is no specific definition of what data may be collected and what data may not, but the data controller or processor must be available to explain the necessity of collection and usage

of certain categories of data. If the service provider keeps more data than is necessary for actual service provision, such keeping is very likely to be unlawful.

The GDPR provides the data subject with the right to be informed of how long data is stored or under which circumstances deleted. Recital 39 of the GDPR states that the period for which the personal data is stored should be limited to a strict minimum. To ensure that data is not kept without necessity the controller should establish time limits for erasure or for a periodic review of collected data [28].

Consent. Under the GDPR processing personal data is generally prohibited, unless it is expressly allowed by law, or the data subject has consented to the processing [28]. This means businesses must request and receive user's consent in order to collect, use, and move personal data. Consent must be asked also for data collecting for advertising, analytics, or crash logging. According to the GDPR consent must be freely given, specific, informed and unambiguous [28]. For consent to be considered freely given, it must be given on a voluntary basis. In order to be informed and specific, the data subject must be notified about the controller's identity, which data will be processed, how used, and the purpose of the data processing. Last but not least, consent must be unambiguous, which means it requires either a statement or a clear affirmative act [41].

For both EU and US consent is an important part of personal data processing. Nevertheless, both use a different approach to gain it. Under EU law opt-in in data collection is required, which means explicit consent must be received before data collection. On the contrary, under US laws opt-out approach is applicable, which mean the user has given the consent to data collection by using the app but can request opt-out from data collection.

Personal data de-identification. Personal data de-identified can be done in two ways: pseudonymization and anonymization. Pseudonymous data is personal data that cannot be attributed to a specific individual without the use of additional information. Anonymous data is stored without any identifiers or other data that could identify the individual or the device to whom the data is related [42]. Pseudonymization can be performed by replacing user names or device information with a pseudorandom number. Anonymization can be performed by removing all the information that can link to a

certain user. It gets much harder to provide real data anonymization if biometric or location data is used since it is hard to remove connections to a single user [43].

Rights of the data subject. The new approach introduced by the GDPR aims to empower data subjects regarding their own personal data, by providing the ability to move, copy, transmit or erase personal data.
Data subject rights aim to give to the data subject control over personal data. In contrast, US law does not have this specific requirement on the federal level and states might have different privacy regulations. For instance, the California Consumer Privacy Act (CCPA) contains the right to access personal data as well as the right to request data erasure. This act, introduced in 2018, will come into force at the beginning of 2020 [44].

Right to data portability. Among other rights, the GDPR introduced the right to data portability. According to the article 20 of the GDPR, data subjects have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format [28]. This right gives the data subject an opportunity to transmit the data to another controller. The Working Party set up under article 29 of Directive 95/46/EC provide data controllers with specific guidelines on how the right to data portability should be implemented into practice [45].

Guidelines give an explanation that data provided by the data subject means not only data actively and knowingly submitted such as name, email, age, address, phone number, but, also, observed data related to the user such as person's search history, traffic data and location data [45].

On user's request this data should be provided without undue delay (no longer than 1 month and up to 3 months in special cases) and free of charge. As a further matter, guidelines state that information shall be provided in commonly used open formats (e.g. XML, JSON, CSV) or other format in common use for a given industry.

US laws, as well as APA assessment list, do not require from service providers to include functionality to export user's data. Nevertheless, if the American company provide services for EU citizen, GDPR requires such companies to be compliant and fulfill the requirement.

Right to erasure/Right to delete data. The article 17 of the GDPR allows data subject to request form data controller personal data erasure regarding himself or herself if: those data are no longer in relation to the purposes for which they were collected, he or she withdraws consent are there is no other legal ground for processing, personal data were collected unlawfully [28].

Nevertheless, the right to erasure is not an absolute right and it has certain limitations. According to the aforementioned article, data shall not be erased if the processing is necessary: for expressing the right of freedom and information, for fulfillment of other legal requirements, for reasons of public interest in the public health area, for scientific or historical research [28]. As it was mentioned above, data subject right to erasure cannot always be fulfilled. For example, medical data cannot be deleted in most cases. Furthermore, if there is a legal reequipment to store data for a certain period of time, a minimum of personal information can be kept, thus fulfilling this requirement. However, if there is no direct legal requirement to keep the data, it should be deleted upon request.

Data sharing. Data sharing means the disclosure of data from one organization to a third-party organization [46]. In any occasion, when data sharing take place there must have a legal basis. That can be consent, contract, the legitimate interest or other legal ground. The same requirement is applicable for data transfer to the third country. If the data is stored in the server, located in another country, the cross-border transmission of personal data takes place. In its article 45 the GDPR sets that this country shall ensure adequate legal protection for personal data [28].

Under the GDPR data subject is in control of his or her personal data. They have the right to know how collected data is used [28], which means if data sharing takes place, the user has the right to know to whom data is shared, what is the purpose and to what extent. According to APA Evaluation Model, users should be informed about personal data sharing, but this does not oblige service providers to give specific information. One of the most recent studies conducted by Huckvale K. et al. (2019) point out that main focus of services provided by Google and Facebook is data sharing with third parties which include linkable identifiers but despite that mobile apps' users are not informed that their data will be shared this way [47]. If a person uses the mobile application it is most likely

his or her data will be shared with Google analytics, Facebook analytics or similar services.

Cookies. Cookies are small data files sent from a website and stored on the user's device. They are used to keep user's login data, settings and preferences which allow to provide a more personalized experience [48]. Cookies and similar technologies exist in mobile apps as well, however, they remain inside the apps and due to that their usage is limited and more fragmented compared to web cookies [49].

Cookies that are stored on a user's device for a set period of time or until deleted. Service providers can use essential and non-essential cookies. Essential cookies have to provide the requested information to the user. All the other cookies are considered non-essential [50].

In EU law using cookies is regulated by the GDPR and ePrivacy directive. The recital 30 of the GDPR states that cookies might be considered as personal importation as long as they provide the possibility for direct or indirect identification of natural person via the device. In the majority of cases, cookies are subject to the GDPR, including cookies for analytics, advertising and functional services. Additionally, the ePrivacy directive requires service providers to give users the opportunity to refuse to have a cookie or similar technologies [51].

To summarize the legal requirements, service providers shall inform users what types of cookies they use and provide an option to decide whether they accept cookies or not. As GDPR is applicable for all entities that provide services to EU residents, web sites and mobile app that can be accessed from the EU have to adopt this policy.

Unlike the EU, US laws do not consider cookies as personal data, however, this approach is changing. The California Consumer Privacy Act consider a device identifier, an IP address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology to be "unique identifier" or "unique personal identifier" [44].

In APA Evaluation Model cookies are considered as one of the evaluation points, however, it does not specify how user needs to be informed. If the service provider uses cookies he needs to inform users about it but it is on provider's discretion in which form (in the privacy policy or app). Also, it is not required to specify what cookies are used.

Data storage. From both GDPR and APA perspective it is important that data is stored securely, and user is informed whether the data is stored locally in user's device, or transferred for storage to the server. However, regardless the place of data storage service provider has to ensure that reasonable security measures are taken to protect users' data from unauthorized access, use, modification or erasure. Furthermore, the article 15 of the GDPR introduce the right to be informed which includes the right to know how long collected data will be stored [28].

Security measures. The GDPR requires entities which are data controllers and processors of personal data to apply technical and organizational measures to ensure proper security level [28]. Safeguarding measures against unauthorized access or unlawful data processing must be sufficient. Implemented measures depend on nature, scope, contest and purposes of processing, as well as risk likelihood and severity. In other words, the more sensitive data are collected and processed the more security measures must be applied.

The article 35 of GDPR provides some examples when processing is "likely to result in high risks" which includes a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, as well as processing on a large scale of special categories. As long as mobile apps make analysis and prediction based on health, personal preferences or interests, reliability or behavior, location or movements or processing data concerning health it is required to take respective measures to protect those data.

The article 32 of the GDPR includes encryption as one of security measures. Encryption is a mathematical function that encodes data in such a way that only authorized users can access it [52]. However, it is important that sensitive information should not be kept as plain text and strong encryption should be used, otherwise, in case of personal data breach or other occasion event, weakly encrypted data can be decrypted by an intruder.

The other important aspect of mobile apps security is to provide a safe communication channel between user and server. Data transmitted via the unencrypted channel, including health-related data, might be hijacked or modified the attacker. Modern technologies allow to secure communication using different methods, for example, Secure Socket

Layer (SSL)/Transport Layer Security (TSL) protocols. SSL and its updated version TSL are a cryptographic protocol that allows secure communication via the network. SSL/TLS protocols used for encrypting information between two points, usually between client and server [53]. TSL allows sensitive information such as login credentials, health-related information, credit card details to be transmitted securely.

Data protection officer. The article 37 of the GDPR contain the legal norm to appoint a Data Protection Officer (DPO) in case if data controller's core activities require large scale, regular and systematic monitoring of individuals or process a large scope of special categories of data [28]. This means if the application uses online behavior tracking DPO appointment is required. Moreover, information about DPO must be publicly available.

3 Methodology

3.1 Research methods

In order to determine the most relevant methods, academic literature was studied. From the literature overview performed for this research, it was found that to provide a legal compliance evaluation of mobile application privacy policy assessment is usually used. The privacy policy is checked against the list of questions defined by the author based on legislation. Some researchers perform privacy policy review as an independent study [20], [54], [55], whereas, others combine it with technical methods [11], [47].

Among technical methods used for mobile apps privacy and security analysis, static code analysis is most commonly used. For example, research conducted by Ferrara & Spoto (2018) show how static analysis can be used for GDPR compliance assessment [56]. To make a comprehensive analysis it was decided to use both methods.

In order to make a comprehensive analysis, evaluation was done in 3 parts as shown on the Figure 1.

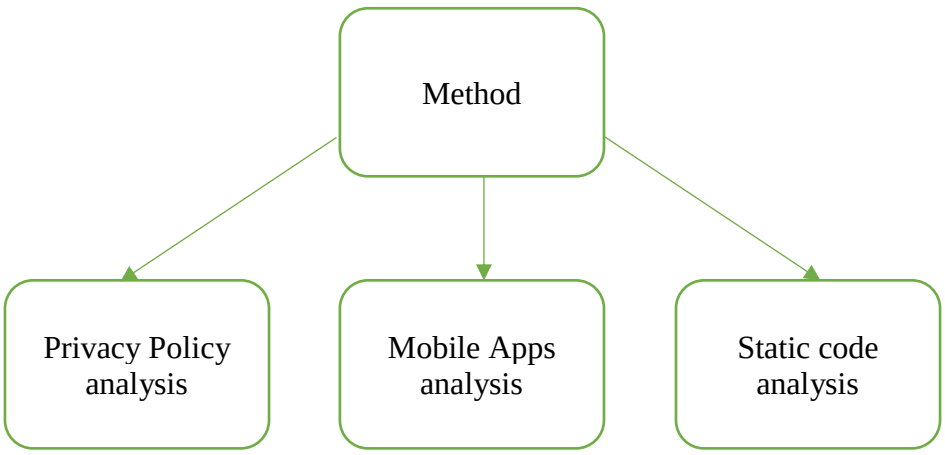

Figure 1. Method

Privacy policy analysis and mobile apps analysis were performed from the user's perspective and no special tools were used. Mobile apps analysis is the evaluation done from a user's perspective to confirm that a statement from privacy policy is implemented in the app. For instance, if the app states that personal data is not collected without users consent the usage of the app shows whether consent for data collection is actually asked. The same rule is applicable to the age check. The privacy policy states the app is for 18+ year-old users, and the use of mobile app helps to define whether age is actually checked, or the user needs to confirm that he/she is 18 years or older.

Nevertheless, certain information cannot be available during app usage. For example, the policy may state that the data is transferred via a secure channel or there is no information about data transmission. To obtain this information static code analysis is used. Static code analysis refers to analyzing the source code of software without executing the software [57]. To perform static code analysis, it is necessary to confirm if the information (especially the one about security measures) provided in the privacy policy is actually implemented in mobile apps' code. Furthermore, static code analysis can provide additional the privacy and security information, hidden from the regular user's eye. In addition, static code analysis was done to confirm the information provided in the privacy policy, to receive more information which is not included there, to identify the most common mobile apps vulnerabilities among mental health apps, and to detect leak of confidential information. Sometimes it is not defined in privacy policy whether the data is shared and with whom it is shared; static code analysis shows this information. As a further matter, static code analysis allows to learn more about the data collection and permission application use (to write to /read from the app storage, to get access to user's location, contacts, photos) as well as about data sharing (ID analytic, advertisement).

In order to make in-depth privacy and security analysis the most suitable frameworks were used. Two evaluation frameworks that represent EU and US attitude towards privacy and security were used for analysis and to compare different approaches. APA App Evaluation Model and GDPR were chosen due to their objective and comprehensive approach to evaluation. Both models are applicable for evaluation of mobile apps that are available directly to users and do not require mandatory health care provider involvement as, for instance, HIPAA. Since APA Evaluation Model does not provide specific requirements, but rather questions, based on which the evaluation can be done, US legal

acts containing privacy and security regulations applicable to mobile apps were used as a basis of analysis.

APA App Evaluation Model created by one of the largest and most respected international organization in the psychiatric field. The model is a hierarchical framework intended to be used specifically to evaluate mobile application related to mental health. The background level of this model is to answer questions about privacy and security, questions provided in the list were used for evaluation. This model was chosen for the present research due to its dedication specifically to mental health apps assessment.

The second evaluation framework was built up based on GDPR requirements. Requirements were summarized in a list and further evaluation was conducted based on this list.

In order to perform comprehensive privacy and security analysis, apps were evaluated from both legal and technical perspectives. In this research applications themselves and their privacy policies were checked against the GDPR requirement and APA privacy and security evaluation list.

The first evaluation model chosen for this research is offered by the leading psychiatric organization in the world, the American Psychiatric Association. APA has more than 38,500 members involved in psychiatric practice and research. As an international organization, APA encompasses members practicing in more than 100 countries around the world [58]. In order to help health care professionals and patients to choose suitable and secure applications, APA released its official App Evaluation Model, which provides step-by-step guidelines in app evaluation.

The evaluation framework aims to guide users towards informed decision making about apps' functionality, usability, privacy and security. The apps evaluation framework is freely available on the official APA web site [59] and includes risk, privacy, and security questions as fundamental questions of the review [60].

This model reflects top priority in the mHealth application. Only those applications that completely fulfill privacy and security requirements might be recommended for further evaluation in terms of evidence-based and usability. Thereby, the APA Evaluation Model

is a framework that offers clinicians and patients possibility to make an informed decision about using the app by answering basic privacy and security questions [60].

As shown on the Figure 2. APA App Evaluation Model is hierarchy-based evaluation framework that includes 5 levels. The evaluation can be done by following these 5 steps:

1. Gather background information
2. Risk/Privacy and safety
3. Evidence
4. Ease of use
5. Interoperability.

Figure 2. APA App Evaluation Model

Each of these five topics contains a list of questions that can be answered by the person who is reviewing the app: physician, patient or both. In the first step of evaluation general questions about the application's business model, developer, platforms used, updates, business model and containing advertisement, should be answered. For app evaluation APA Risk/Privacy & Security mobile apps Evaluation model [59] is used and includes following question:

- Is there a privacy policy?
- What data are collected?
- Are personal data de-identified?
- Can you opt-out of data collection?
- Can you delete data?
- Are cookies placed on your device?

- Who are data shared with/What data are shared?
- Are data maintained on the device or the web (i.e., “the cloud”)? Both?
- What security measures are in place? Are data encrypted on the device and server?
- Does it purport HIPAA compliance? / Does it need to be HIPAA-compliant?

Since this research is focused only on privacy and security evaluation, the step regarding risk/privacy and security was used. According to the APA, mental health apps should be evaluated before implementation into the treatment process. The rate provided by users in the app store cannot be completely trusted since it displays subjective users experience feedback, not an objective evaluation.

APA states that apps may not be secure in the way that personal health data entered by users may be easily accessed by others and improperly disclosed. Moreover, many apps may sell patient collected data without informing users about this [61].

The GDPR evaluation list was build up alike APA Evaluation Model, additionally considered GDRP specific requirements. For GDPR compliance evaluation GDPR requirements applicable for mental health mobile apps, were added. The following points were estimated:

- Provide services to EU residents;
- Have policy;
- Collect personal data;
- Explicit consent to process personal data;
- Inform users how their data might be used;
- Inform users where the data is stored;
- Transfer personal data to third countries;
- To whom is shared;
- Age check (minors);
- Edit profile;
- The right to the data portability (import data);
- The right for erasure (delete data);
- Information about DPO;
- Cookies;
- Security measures.

3.2 Apps selection process

A structured review process was used to guide the collection of apps. The process of apps selection is shown on the Figure 3. Apps selection process.

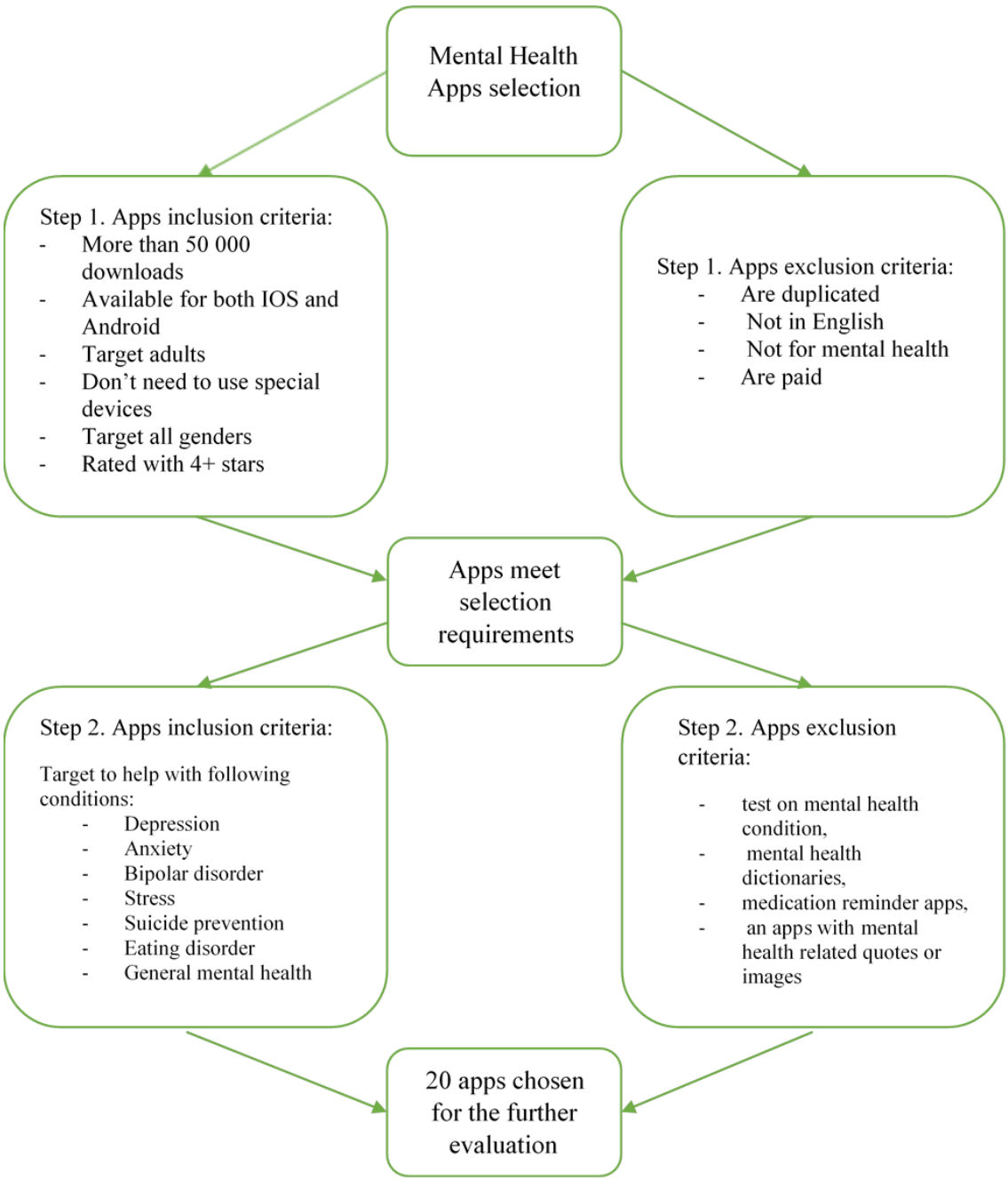

Figure 3. Apps selection process

The goal of apps selection process is to include in the analysis free application available for both Android and IOS platforms, with the highest rate, the biggest number of downloads, aiming to support people with different categories of mental conditions. Applications were chosen and retrieved in February 2019.

In order to find a mobile application suitable for current research were used Google Play Store was used for Android apps and Apple App store was used for IOS apps. By performing a search with “mental health app” and filtering by “free” and “4 stars+” 250 applications were displayed in each store; only apps that do not need to be connected with any special devices were chosen for this research. Basic application overview by name and description allows to add application into the category according to the conditions they aim to help cope with. To the most common mental conditions were used to split apps into the following categories:

- Depression
- Anxiety
- Bipolar disorder
- Stress
- Suicide prevention
- Eating disorder
- General (online consultation)

Applications in different categories were chosen by using keywords “depression”, “anxiety”, “bipolar disorder”, “stress”, “suicide prevention”, “eating disorder” respectively. Additionally, results from general “mental health app” search target non-specific mental condition were added. Some apps fall into 2 or more categories, they were added to the more relevant category. The applications which aimed to provide a test on having depression, anxiety or other health condition, mental health dictionaries, that describe symptoms only, medication reminder apps, an application that provide mental health related quotes or images were eliminated. In total, 20 top rated application were selected for research.

3.3 Environment installation and evaluation process

In order to make a comprehensive analysis, evaluation for the present research was conducted:

1. From a user perspective – app's privacy and security and privacy policy analysis, excluding the use of additional tools;
2. Static code analysis – including the use of additional tools.

In order to perform the first part, user perspective analysis, 6 steps were followed as highlighted on the Figure 4. Applications were downloaded and installed on the mobile device. Privacy policies were accessed directly from applications or respective web sites. Privacy policies content was analyzed based on APA and GDPR requirements. User's account was created in applications where possible. During the registration and usage, the following questions were answered:

1. What data the user is asked to input to start using the app;
2. Whether the user is asked to input sensitive personal data such as health care, race, sexual orientation related data) or not;
3. Whether the user is asked to give consent before data collection and whether the consent can be withdrawn;
4. Whether the user is informed about the use of cookies or not;
5. Whether the user's age is checked or not;
6. Whether it is possible to edit submitted information;
7. Whether it is possible to export user's data from the app;
8. Whether it is possible to delete user's data.

For the purpose of the user perspective evaluation, apps were used during one month period of time. In order to export the data, inbuilt app functionality or the possibility to send the request to the application provider was used (in case of incapability to export the data directly). In the final step of research, user account was deleted from the app or request to delete was sent to the app provider. After two weeks an attempt to log in using the same credentials was made to check whether the user account was actually deleted.

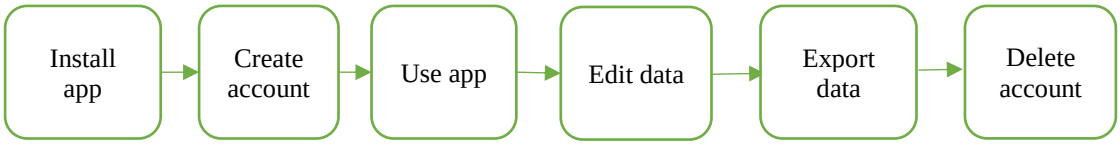

Figure 4. Steps in app evaluation from user's perspective

The second part of the evaluation, static code analysis, is one of the main tools for application privacy and security risks assessments.
During static code analysis following questions were answered:

1. Which permissions application use and whether they are necessary for app functionality;
2. Does the app use third-party libraries and whether they are safe;
3. How the data is stored;
4. Whether the data is transmitted via a secure channel;
5. Whether the encryption is used, and is it strong enough;
6. Whether the app is capable to define device location.

For static analysis Kali Linux 2019 was used on Oracle VM Virtual Box 6 installed on Windows 10 Operating System. The extracted java source code was read using IntelliJ; MobSF v. 1.0 was downloaded and installed on Kali Linux. MobSF is a free mobile security framework which includes tools that can be used to perform static and dynamic code analysis for Android and IOS applications [62]. MobSF was used in order to automatically decompile (extract the source code) the Android Application Package (APK) - package file which contains all the components of Android application including activities, services, broadcast receivers and content providers; read the Manifest file, where all app components are declared, identify issues in the source code and in the Manifest file, and extract the certificate of the application.

To conduct this study, Android apps were chosen due to the following reasons:

1. Easy access of applications' APK files
2. Less obfuscation
3. Root access to the device
4. Easy to decompile

Google Play Store does not perform manual apps testing or reviewing for approval, only automated malware scanning. Consequently, Android apps may expose a risk to the users. Moreover, Android devises allow to install apps from sources other than Google Play Store, such as third-party websites and torrents. Such level of freedom opens new opportunities to the attacker by modifying a widely used app with a malicious piece of code, upload to unofficial resource and thus the collect user's data.

In order to start with the apps' analysis, APK files of selected apps were downloaded from the official Google Play Store. MobSF was able to decompile APK files and inspected all of the 20 apps. MobSF automatically analysis APK and provide information about: apps permissions, list of activities, domains to which application is connected, use of 3rd party libraries, containing possible vulnerabilities and malware. Reports created by MobSF in PDF format were downloaded. Additionally, online scanner HTBridge was used to confirm findings form MobSF. Java source code extracted by MobSF was downloaded and manually analyzed in order to see finding in context and to exclude false positive findings.

Static code analysis was performed by following steps as highlighted on the Figure 5.

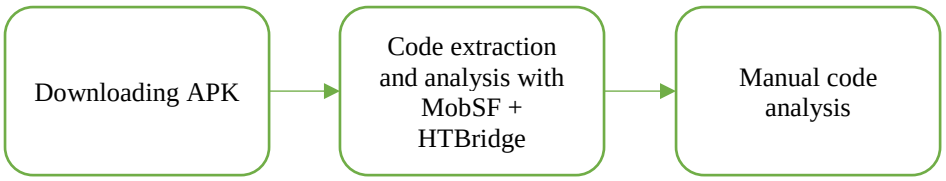

Figure 5. Static code analysis

4 Results

The present chapter explains the results of the mental health mobile apps analysis based on the GDPR and APA requirements. Since this research is intended to detect tendency and patterns regarding noncompliancy rather than evaluate specific apps, in the presentation of results the applications are pseudonymized by substitution to alphabetic letters.

In total 20 applications were analyzed for this research. 14 apps out of 20 allow users to create an account and collect personal data from users, such as name, email, date of birth, country, 2 out of which apps may collect personal data if certain features are used or the application is connected to social media. 6 apps do not provide an option to create a personal account or connect via social media and data collection is limited to technical information, such as device type, IP address, browser, OS, Internet service provider.

The initial step was to identify whether the app collects personal data from APA and GDPR perspective. APA consider as personal data information about a natural person, not a device, which means personal data collection is linked to the personal account in the app. The GDPR provides a much wider approach and include regarding personal data and include digital identifiers to this definition. In certain cases, mobile apps state that they do not collect information that can directly link to a natural person, but in reality, they do collect the data which is actually considered under GDPR as personal. The mobile applications privacy policies provide users with information about what data are collected, how it is stored and handled, to whom it might be shared. Both guidelines the APA assessment and the GDPR pay attention, whether apps have a privacy policy or not.

Privacy Policy. Having a privacy policy is one of the most important requirements for an app that collect user's personal data for both APA and GDPR assessments. The vast majority of apps (17 out of 20) have a privacy policy, as shown below on the Figure 6.

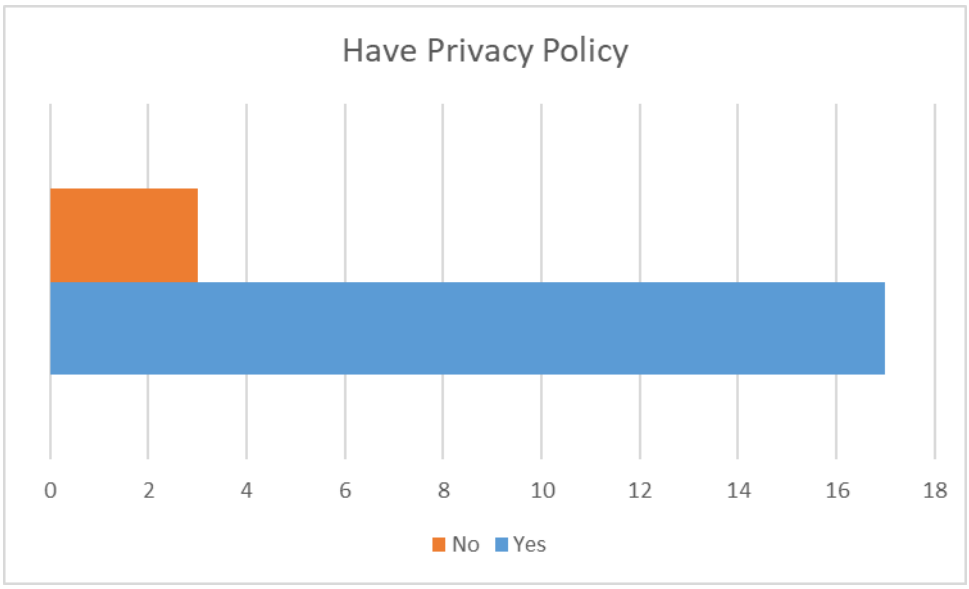

Figure 6. Privacy Policy

All of those policies are available in English. The privacy policy must be easily accessible for users, which is not always the case. Some services published a privacy policy on the web page, but not in the app. It is required that privacy policy must be specific. Unfortunately, 5 out of 20 apps do not follow this requirement and use general phrases to describe their activity. Instead of providing the users this the list of data which is collected (name, email, address, phone number) it may just state “collect information that you provide us”.

In many cases, the policy covers not only use of the mobile app but service, in general, and thus may include additional paid services such as a consultation with a specialist, purchasing via the app or using of the web application. If businesses do not separate in privacy policy how they process personal and non-personal data, will lead to a certain confusion for users, and consequently, constitute a violation of the requirement that information provided to the user must be presented in clear and unambiguous way. 3 applications without privacy policy do not collect data about a natural person directly from users. Furthermore, one of for the applications (app “A”) claim to have a privacy policy, but it cannot be accessed for users due to the unsecured connection, blocked by the browser. For this reason, it is marked as “no privacy policy”. If an application does not collect personal data which can directly identify an individual, there is no requirement to provide users with a privacy policy, which consequently means none of 20 violate privacy under the APA approach.

In order to be GDPR compliant, the mobile application should inform users about data collection. Whether it is personal information about a natural person or technical information about the device from which app is assessed users have the right to know. Considering the aforementioned, all of 20 apps, chosen for this research need to have a privacy policy, which means that 3 out 20 violate GDPR requirement. In addition, 2 more apps have a privacy policy *de jure*; however, *de facto* these policies do not provide users with the required information.

Data collection. 16 apps collect or might collect personal data, about a natural person such as name, date of birth, contacts, location, health-related information, all of 20 apps collect at least minimum of technical data about user's device, as illustrated on the Figure 7.

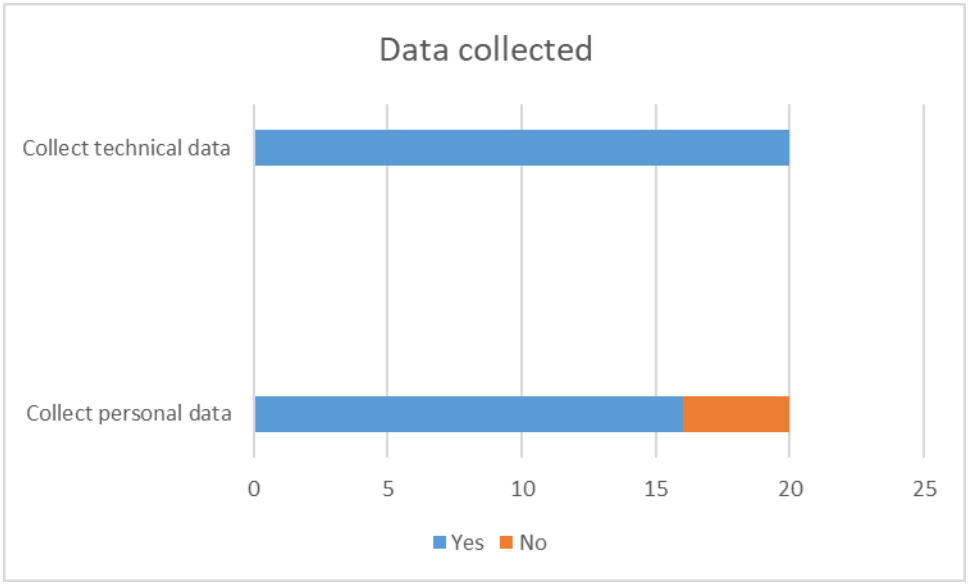

Figure 7. Data collected

Consent. 16 apps ask for consent for data collection form users, as illustrated on the Figure 8, but only 7 of them ask for explicit consent where the user has to agree actively, for example by ticking the box as required by the GDPR. 9 apps use an opt-out approach, by informing users that they give consent by using provided service or submitting personal data. These apps informed the user in the following manner "by submitting your personal information you consent to the collection and processing of your personal information"

or “by using service you a agree to terms of use/privacy policy”, which cannot be considered as explicit consent. 4 apps do not provide any information or ask about consent, 1 app informs the user about rules regarding using the app, but does not inform about personal data processing. Moreover, 1 of those apps collects from users’ personal data such as name and email.

Speaking about other application, that does not provide personal account registration it becomes not that straight forward to distinguish whether they collect personal data or not. For example, the app “J” state in its privacy policy that it does not collect any data that allows a direct person identification. Nevertheless, app “J” informs users that data is stored on private servers and that user’s personal data may be transferred to third parties in the United States while using their third-party tools. Based on the aforementioned and considering applications’ functionality, it is possible to conclude that, in fact, personal health-related data is or might be collected.

Moreover, applications do collect technical information about the user’s device, including “Identifier for Advertising in Apple” for iOS devices and “Advertising ID” for Android devices. Additionally, the static analysis showed that GPS function is also available via the app “J” application. Thus, it is possible to assume that the combination of all that data may lead to specific devise identification and consequently, identification of a natural person - the user of that particular device. App “J” provides the following information about consent “We do not pass on your data to third parties, unless we are legally entitled or obliged to do so, or you have given us your consent. We transmit your health data in the context of research cooperation in a completely anonymous form to the above-mentioned universities” but in fact, the user was never asked ask for consent.

However, app “Q” despite collecting personal data, including health care data, that belong to the category of sensitive data, neither inform users about data collection, nor ask for consent. 11 apps provide an option to opt out from anonymous tracking, sharing data with a third party, marketing, unsubscribe from newsletters. At the same time, the app “T” notifies users that even if they opt-out, the service may still collect and use non-personal information regarding users’ activities.

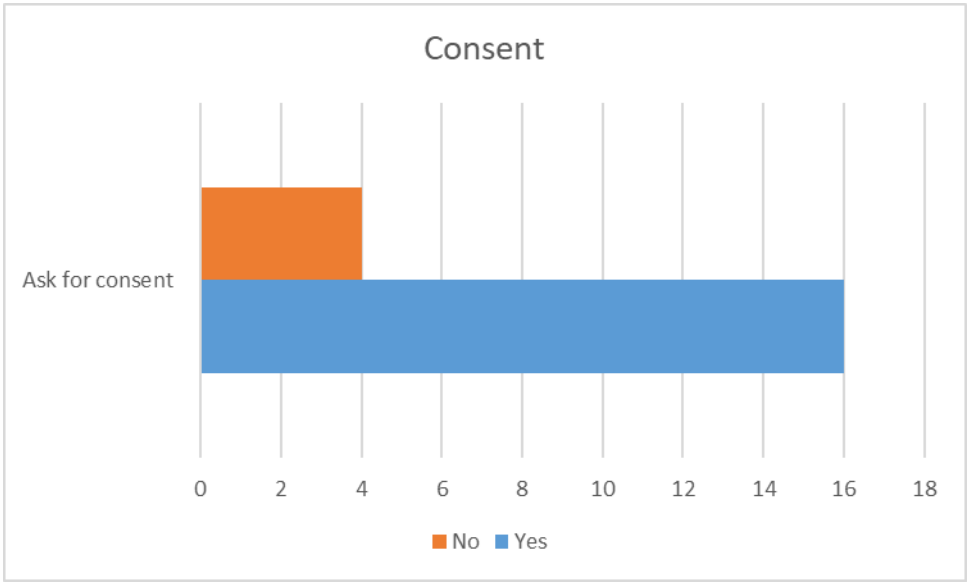

Figure 8. Consent

Personal data de-identified. All 14 apps that collect personal data such as name, email, health-related data state in their privacy policies that they use anonymization or pseudonymization for activities in which they do not require personal identification. Non-identifiable information might be used for research, marketing, and service improvement purposes.

Rights of the data subject. Right to data portability. 16 out of 20 analyzed apps fulfill data portability right by allowing users to export data; 15 of them provide data in commonly used format such as CVS, JSON and XML, but 1 app use application specific format, which cannot be read by the commonly used program. App "N" provides users with guidance on how the data can be downloaded via the web application; the data, however, was not accessible following provided guidelines. There was no answer received for further user's request. App "H" reply to a user request to export data, that since user do not proceed with this paid functionality, all data was deleted. However, it was possible to login using the same credentials and assess personal account via the app, which shows that actually data was not deleted as informed. For other 2 applications which work like an informational resource, this requirement is not applicable due to the absence of online entries.

Right to erasure/Right to delete data. 17 out of 20 apps, including 4 apps that do not provide the possibility to create an account, but allow to make online entries (mood rate, diet notes, uploading pictures) enables to delete the data via the application by themselves

or upon email request, as illustrated on the Figure 9. For 2 apps which function more like informational resource and do not provide an option to download any data, this reequipment is not applicable.

Moreover, the privacy policy of the application “H” states that private health data cannot be erased upon a user’s request, because of US law required to keep medical records for 7 years. App “I” allows to delete the data, but warn that certain information can be kept for recordkeeping purposes. 17 application state in their privacy policy, that data can be deleted upon request or have “delete account/data” button, however only 13 of them actually deleted the account/data. The GDPR set a limit of one month to fulfill the user’s request. Nonetheless, in the case of 4 apps, one month after sending the request it was still possible to log in using the same registration credentials and access online entries.

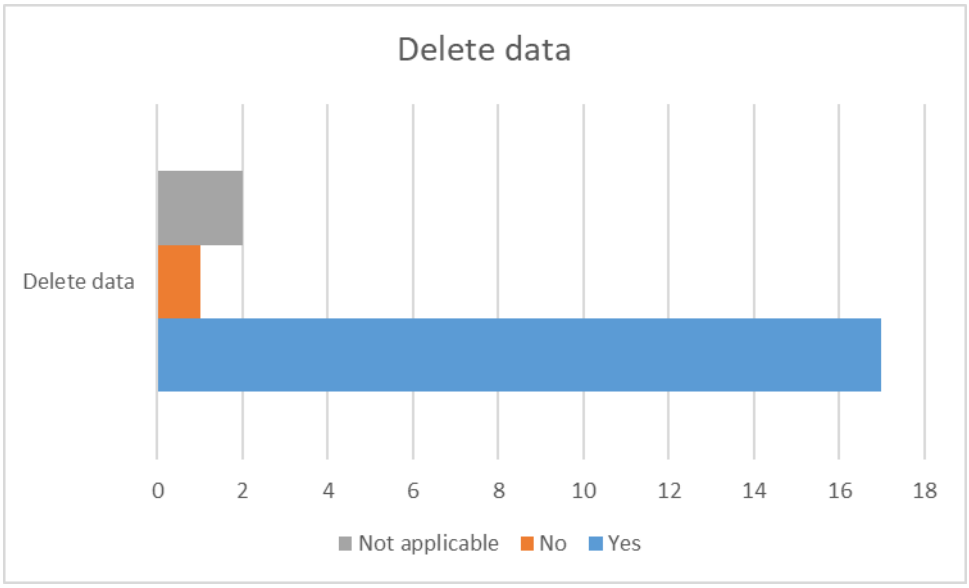

Figure 9. Delete data

Data sharing.17 out of 20 apps admit they may share data with third parties. It can be related to the nature of services provided, for example, sharing personal data with a therapist for teleconsultation, with a credit card payment provider for payment processing or with data storage providers. Also, anonymized or pseudonymized data might be used in for the research, analytics, marketing or other purposes. 3 other apps do not have a privacy policy and do not inform users directly via the app consequently users are not aware if data sharing takes place. Static code analysis showed that 18 apps share user’s data with analytic services such as Google analytics, Facebook analytics and Firebase,

however, only 11 of those apps inform users about sharing data with 3rd parties, and that might not be directly related to the offered service itself. 6 of those apps provide more specific information about with whom the data is shared and what is the purpose of sharing.

Cookies. According to the information provided in privacy policies, 14 apps use cookies, other 6 apps to do not provide information whether they use cookies or not. Since APA Evaluation Model does not provide any additional requirements, these 14 fulfill the requirement. However, code analysis showed that the rest 6 apps also use cookies or similar technologies, but do not inform users in any manner.

Besides informing the user, EU legislation demands receiving consent on using cookies. According to the legal requirement, users have to be given the right to accept or deny cookies. Only 5 apps display a message about using cookies within the application and allow to choose whether the user agrees with this or not. Others apps provide no information about using cookies (4 apps) or do it in privacy policy only (11 apps) which leaves no possibility to decline cookies.

Data storage. 6 applications store data in user's personal devices only, 3 apps use both device and server storage, 10 apps store data on servers. 19 applications provide information about the data storage in the privacy policy or within the application and 1 app does not provide any specific information about the data storage.

Security measures. In both APA and GDPR assessments special attention is paid to security measures. According to the APA Evaluation Model, it should to be considered what security measures are in place and whether the data is encrypted. Nevertheless, standards and requirements are not set. The GDPR is more specific about security measures that shall be implemented; for instance, encryption and secure communications channels for data transmitting shall be used.

From a regular user's perspective, privacy policy and the actual use of the application are the only sources to get information about what is done by the service provider to make an app secure.

According to the apps privacy policies the most widely used security measures are encryption (used by 10 apps), password or PIN code (15 apps), secure communication (8 apps). In other apps that have privacy policies, it is either not mentioned what security measures are used or they are described in a very general manner for instance that commercially acceptable measures or industry standards are used, without providing specific examples. Moreover, certain apps mention that despite using preventive measures transaction via the Internet cannot be 100% secure and any transmission is made at user's own risk.

Authentication is an important part of security measures. Proper user's authentication allows to prevent unauthorized access to personal data including sensitive data.
Based on information written in privacy policies and user's experience, it was found that 14 out of 20 apps use password or PIN code to secure the data. Additionally, 8 allow users to set a fingerprint as authorization method, including 1 app , that uses a fingerprint as the only option to get access. However, neither the privacy policies mentioned this authentication method, nor specified how retrieved fingerprint data is stored or might be used.

Less than half of apps (8 out of 20) specify in their privacy specify that secure connection is established. Static code analysis confirmed this statement. Although other apps do not provide information about the connection, static code analysis showed that 7 more apps use secure connection. Summarizing findings from privacy policies and static code analysis 15 out of 20 apps use a secure connection.

During security measure evaluation other important issues, which deserve special attention, were found. Additional security risks occur when apps use 3rd party libraries in their source code. It is safe to use libraries from trusted sources, however, unknown libraries may contain malicious code and its implementation may lead to the app's misuse without developer's knowing about it.

According to the GDPR requirement, only data that is needed for service provision shall be collected. In case of mobile application, besides information directly provided by the user, it is important to pay attention to apps' permissions, that allow to access user's device storage, camera, location, and to record audio. As it is shown on the Figure 10

many applications may ask for permissions, which are not directly connected to the offered services. 15 apps, including 3 apps with no user account allow to access user's location. In some cases, in-build packages *com.google.android.gms.location* or similar contain the various function of location services which cannot be manually turned off by the user.

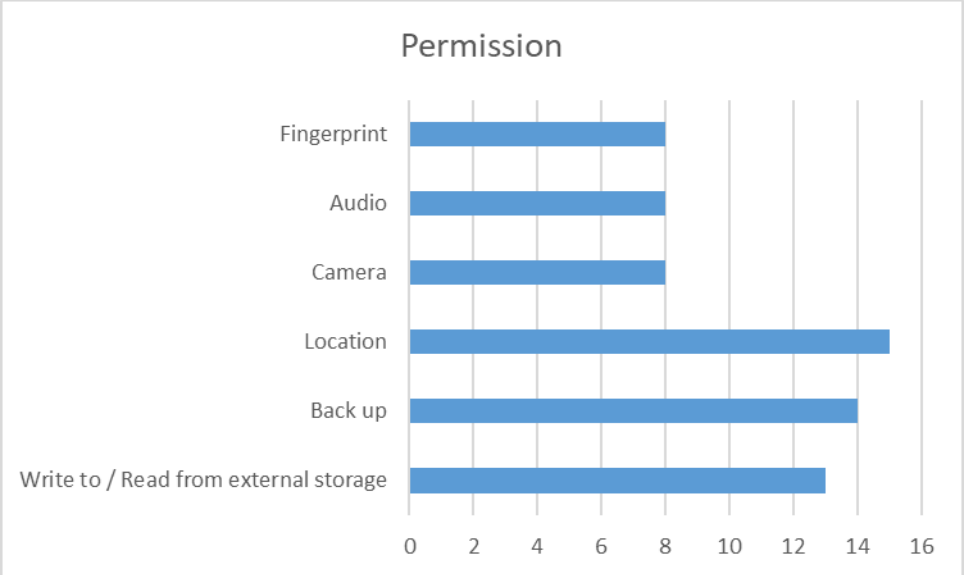

Figure 10. Permission

APA App Evaluation Model recommends scoring apps as "appears ok", "some concern" and "bad". There are no certain criteria how to score apps, however, it is mentioned that if the privacy policy does not answer questions provided in evaluation list or there is no privacy policy at all, this particular app cannot be considered as safe. Each application was given score "1" for fulfilling requirement, "-1" for violating the requirement and "0" for a partially fulfilling requirement. For example, "1" is given when there is privacy policy "-1" if there is no privacy policy, but it is required, or privacy policy is not accessible for users and "0" if there is privacy policy but its quality is poor and it does not provide required information.

Since APA and GDPR have different requirements evaluation score was given separately. APA and GDPR score assignment are shown on Table 1 and Table 2 respectively. Apps with the highest score are marked with a green color and apps with the lowest score are marked with an orange color.

Evaluation score based on the APA and GDPR frameworks is shown on the Figure 11 and Figure 12. Since APA and GDPR have a different number of requirements, the highest score per application is also different. In APA evaluation the highest point in 7, and in GDPR it is 10.

Table 1. APA score

App	Privacy policy	Consent	Personal data de-identification	Edit data	Delete data	Data sharing	Security	Total score
A	-1	0	1	1	1	0	-1	1
B	1	1	1	1	1	1	1	7
C	1	1	1	1	1	1	1	7
D	1	1	1	1	1	1	1	7
E	1	1	1	1	1	1	-1	5
F	1	1	1	1	1	1	1	7
G	1	1	1	1	1	1	1	7
H	1	1	1	1	-1	1	1	5
I	1	1	1	1	1	1	1	7
J	1	1	1	1	1	1	1	7
K	1	1	1	1	1	1	1	7
L	1	1	1	1	0	1	-1	4
M	1	1	1	1	-1	1	1	5
N	1	1	1	1	1	1	1	7
O	1	1	1	1	1	1	1	7
P	0	1	1	1	1	1	1	6
Q	0	-1	1	1	1	1	1	4
R	-1	0	1	1	1	0	-1	1
S	-1	0	1	1	1	0	1	3
T	1	1	1	1	-1	1	1	5

Table 2. GDPR score

App	Privacy policy	Explicit consent	Personal data de-identification	Edit data	Delete data	Age check	Export data	Data sharing	Security	DPO	Total score
A	-1		0	1	1	0	0	-1	-1	0	-1
B	1	1	1	1	1	1	1	0	1	1	9
C	1	1	1	1	1	1	1	1	1	1	10
D	1	1	1	1	1	0	1	1	1	1	9
E	1	0	0	1	1	0	1	0	-1	0	3
F	1	1	1	1	1	1	1	1	1	0	9
G	1	0	1	1	1	0	1	-1	1	1	6
H	1	1	1	1	-1	1	-1	-1	1	-1	2
I	1	1	1	1	1	1	1	1	1	-1	8
J	1	0	0	1	1	-1	1	1	1	1	6
K	1	0	1	1	1	0	1	1	1	0	7
L	1	0	0	1	0	0	0	1	-1	0	2
M	1	1	1	1	-1	1	1	0	1	-1	5
N	1	0	1	1	1	1	-1	0	1	0	5
O	1	0	1	1	1	-1	1	1	1	1	7
P	0	0	1	1	1	-1	1	-1	1	0	3
Q	0	-1	1	1	1	-1	1	1	1	-1	3
R	-1	0	0	1	1	-1	0	-1	-1	0	-2
S	-1	0	0	1	1	-1	0	-1	1	0	0
T	1	0	1	1	-1	1	0	1	1	-1	4

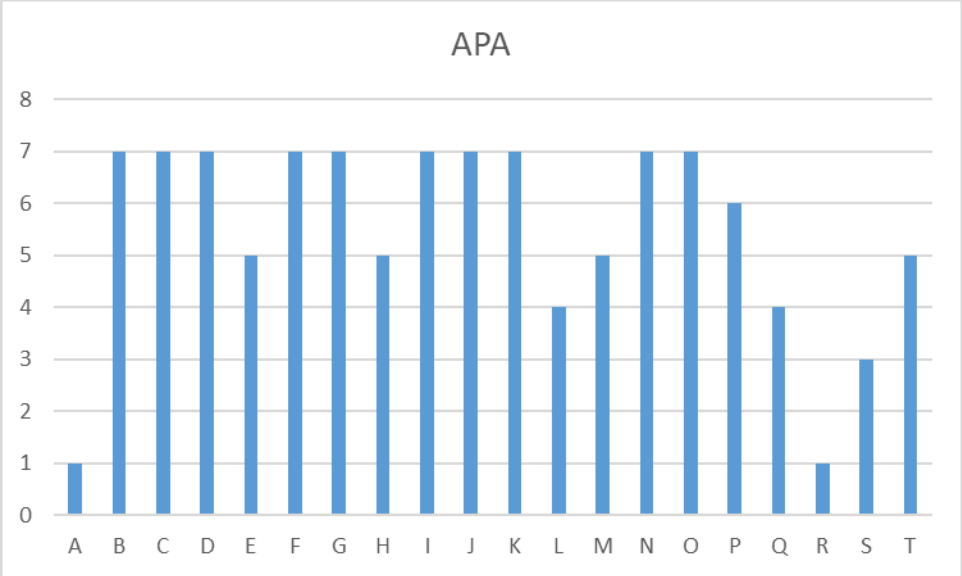

Figure 11. APA compliance score

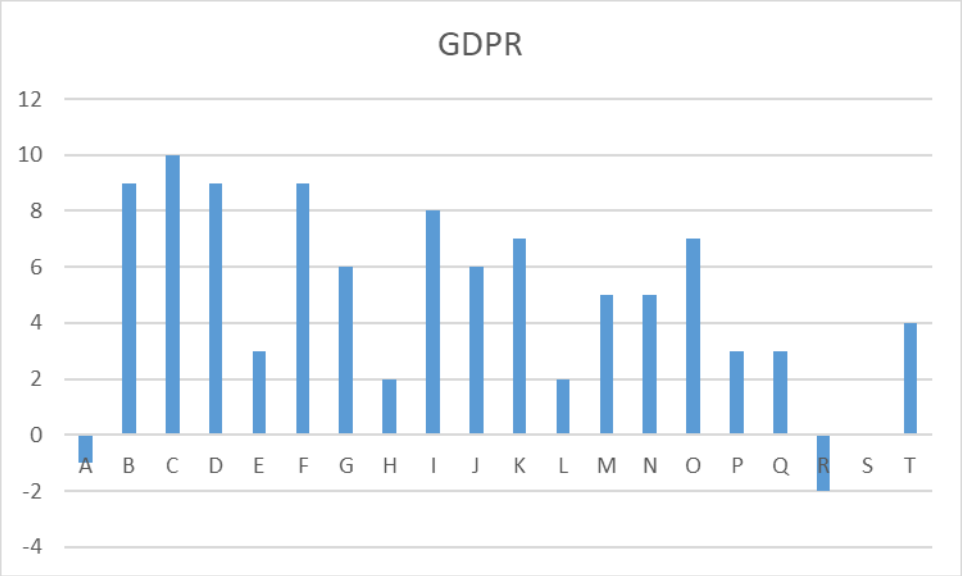

Figure 12. GDPR compliance score

5 Discussion

5.1 Discussion of the key findings

Results of mental health mobile apps analysis showed significant privacy and security concern: most of the applications have one or more privacy and security violations. Only 4 out of 20 apps (20%) can be considered as GDPR compliant and 10 apps (50%) can be considered acceptable according to APA Evaluation Model.

Result of such kind occurred due to the different approaches to mobile apps privacy and security in EU and US. The main difference is about understanding of what should be defined as personal data, and further analysis depends on this definition. According to US legislation and APA Evaluation Model, online identifiers collected by apps are not considered as personal data, meaning there are fewer requirements to privacy and security measures that must be implemented. All analyzed applications fall within the scope of the GDPR, meaning they are bound by the law to implement respective measures.

In general, compared to APA evaluation model, GDPR in more demanding in terms of privacy and security, and its scope of requirement is also wider. However, the US attitude to privacy and security is changing, at least in California. Starting from 2020 the California Consumer Privacy Act, new privacy legislation, comes into force; the Act will introduce a similar approach to understanding online identifiers as personal data.

Furthermore, the GDPR introduces the right to data portability, while there is no such requirement by US legislation or APA Evaluation Model. However, according to the CCPA users will have the right to access personal data which as alike to the right to data portability.

Also, the GDPR unlike US legal acts, has additional requirement to appoint DPO and provide users with contact details.

The next difference is about the scope of data collection. Under the GDPR only necessary minimum data shall be collected by the service provider. At the same time, US legislation does not have such requirement and the scope of collected data it mostly self-regulation for the companies.

25% of analyzed apps appeared to have a non-transparent policy or no policy at all which is not acceptable for mental health mobile apps, since users are not informed about data collection and use. The other common violation is absence of asking for consent – only 7 applications ask for explicit consent to collect personal data, required by the GDPR. One of the major problems is that apps collect more data besides voluntarily given by the user and this data collection about users' devices and online activity in case 20% of analyzed apps happen without informing users. Data transmission to a third party was detected in 18 apps, however, only 7 of them inform users that data sharing take place. This amount is huge, considering that the most highly rated apps were chosen for analysis, those which are considered to be the best.

As a further matter, the common problem is a difference of statements in the privacy policy and real implementation. Although the information may be provided in the privacy policy, apps fail to display that cookies are used and to check users age. The same situation is with the right to export and the right erase the data – those rights exist in the privacy policy, however, are not actually fulfilled in the application. Besides that, mobile apps violate data minimization principle by using unnecessary permissions such as geolocation (15 apps) or camera (8 apps), which are not related to the services they provide. In 70% of analyzed apps information about data protection officer which must be presented in case mobile app processes a large scope of special categories or monitor user's online activity, is missing.

During mental health application certain security issues were detected as well. It was found that 4 apps use weak encryption and unsecure data transition including for user's passwords and sensitive personal data. As a further matter, many applications use 3rd party libraries including unknown and potentially dangerous.

Among main findings other privacy and security related issues were discovered. Two of the analyzed apps were not updated for a long period of time. One of the apps was updated more than 4 years ago, other one – 2 years ago. Technologies are developing, threats are

also becoming more sophisticated, which means even if privacy and security measures were sufficient at that time most likely they are not to ensuring required privacy and security level as of today.

The majority of privacy and security violations were found in apps that are supposed to be anonymous, but still collect online device identifiers. These apps appear to be insecure mainly because:

- Of the lack of transparency about what data is collected and how used;
- Might collect lots of data: location, device identifier, have access to other apps, permission to write to and read from external storage;
- They use weak security measure;
- They use analytics services without informing users.

As discussed above, it is vital for mHealth applications to have a privacy policy; mobile apps that do not have privacy policy should create one and make it available for users. Mobile apps that do have a privacy policy, but the latter is not accessible via unsecure internet connection must fix this issue and make the document securely accessible. In addition, if the privacy policy is too general or contains unambiguous information, it should be clarified.

It is not necessary to have a user's account to identify a certain person using the app with a mobile device. For example, an application collects device information and location from the user, collect user's behavior via using the app and share this information with analytic and advertisement services like Google, Facebook and Firebase. The same user has Google or Facebook account and accesses them using the same device. After some time of using the mobile app, a paid feature of this app appears as Facebook advertainment on the same device, despite different user's credential were used in app and Facebook. This means a combination of collected data can potentially lead to user's device identification, and since usually in the modern word this device is personal, can lead to the identification of a natural person as well. For this reason, the applications should apply respective security measures regardless can the personal account be created or not.

Some applications specify that data is stored unless deleted. Nevertheless, many users create accounts, at some point stop using them, but forget to delete the account. From a

service provider perspective, to fulfill the requirement of data minimization it would be a good practice to inform the user that after some time, for example, 1 year of inactivity the account will be deleted, and user's data erased, unless the user request to keep it.

It was found that 7 apps which use secure connection do not inform users about how the data is transmitted, it is recommended to add this information to the privacy policy and make it available for users. 5 apps which do not use a secure connection for data transmission must establish it and make changes to the privacy policy as well.

This research showed similar results compared to the studies that have been conducted by other researchers, which again stress the problem of privacy and security in mental health mobile applications.

Quality control for this research was implemented in all stages: choosing methods, gathering data, validation of results. Quality assurance was achieved by using methods which have been validated to use for similar studies. In order to ensure the quality of gathered data applications for analysis were retrieved from the official source Google Play Store. In addition, to ensure that static code analysis results are valid additional manual check was conducted.

Results of this thesis are useful for psychologists and psychiatrist and their patients who are considering to use apps in addition to therapy to be familiar with potential risks. Moreover, results may be used by health mobile apps developer for better understanding of common privacy and security problems and for building a compliant application.

5.2 Limitations

Methodology used for this research is comprehensive and includes legal and technical aspects in mobile applications analysis, however, it has some limitations.
Certain requirements, such as information regarding data storage cannot be checked. Methods used allow to analyze if the users are informed whether the data is stored securely, physical safeguarding measures are implemented, anonymization and pseudonymization is used. However, it is impossible to check whether those measures are indeed implemented. The technical analysis for this research was limited to static code

analysis, yet, dynamic analysis, where code is analyzed during execution was not included.

5.3 Further research

For future research, dynamic analysis may be performed to evaluate the apps in terms of privacy and security during data transmission via the Internet and to discover vulnerabilities that expose threats to privacy and security of the application.

Mobile application privacy and security is a process, not a condition. For an app, there is nothing that can be achieved once and last forever. It is a constant work to keep the app compliant.
Following steps can be undertaken to improve current situation and elevate it to a qualitatively new level:

- Contact an application provider and inform about problems and incompliances they have;
- Provide a follow-up research to see whether they manage to fix issues.
- Create an automated tool for mobile apps compliancy evaluation.

Certain steps of the present research such as privacy policy analysis, were performed manually; in future it might be possible to create an automated tool, that extracts and analyzes the information. Moreover, it will be a useful to have such automated tool for comparison of different versions of privacy policies, if service provider makes changes to understand what exactly is a different.

6 Summary

The present master thesis is a practice-oriented study the main aim of which was to analyze the top-rated mental health mobile applications in terms of privacy and security based on APA App Evaluation Model and GDPR requirements. In order to do so, the author of this thesis determined whether the most popular mental health mobile apps are GDPR compliant; whether the most popular mental health mobile apps acceptable in terms of privacy and security from the APA perspective; discussed what are the main problems with apps, which are not GDPR compliant and APA acceptable. For these purposes mobile applications (N=20) were downloaded; implementation of legal requirements and statements from privacy policy into practice were checked using applications installed on the device.

Findings of the thesis show that only half of the analyzed applications is acceptable according to APA evaluation framework and even less, 20% can be considered as GDPR compliant. The low level of privacy and security has been associated with a lack of supervision for mental health mobile applications. These results raise a big concern regarding mental health apps privacy and security in general.

It was discovered that the lack of transparency leads to the biggest privacy and security concern related to the scope of data collection and sharing. Results of the in-depth analysis showed privacy abuse from the application side by collecting unnecessary personal data and using permissions not related to the service itself. Furthermore, the analysis showed that positions related to users' rights exist in the privacy policy, are not always fulfilled in the application.

Contribution of the present thesis is to increase awareness regarding concerns related to the mental health mobile applications privacy and security Highlighting these concerns is the initial step towards increasing privacy and security level and overcoming issues under discussion.

Summing up, it is necessary to state that the research conducted within the framework of this master thesis helped to gain a deeper understanding of problematics of mental health mobile applications privacy and security; the latter undoubtedly should be significantly improved to reach the acceptable level.

References

[1] "325,000 mobile health apps available in 2017 – Android now the leading mHealth platform," 07 November 2017. [Online]. Available: https://research2guidance.com/325000-mobile-health-apps-available-in-2017/. [Accessed 25 March 2019].

[2] "Why choosing a mental health app is harder than you think," [Online]. Available: https://www.nbcnews.com/know-your-value/feature/why-choosing-mental-health-app-harder-you-think-ncna832051. [Accessed 25 03 2019].

[3] "Top 10 Mental Health Apps," Psychiatry Advisor, [Online]. Available: https://www.psychiatryadvisor.com/slideshow/slides/top-10-mental-health-apps/. [Accessed 01 April 2019].

[4] Giota, K. G., George K., "Mental health apps: innovations, risks and ethical considerations," *E-Health Telecommunication Systems and Networks 3,* vol. 3, p. 19, 2014.

[5] G. Atlas, "Mental Health Apps Are Not an Adequate Substitute for Human Interaction," The New York Times, 21 December 2015. [Online]. Available: https://www.nytimes.com/. [Accessed 24 April 2019].

[6] J. Shelton, "Top 25 Best Mental Health Apps: An Effective Alternative for When You Can't Afford Therapy?," Psycom, 24 April 2018. [Online]. Available: https://www.psycom.net/25-best-mental-health-apps. [Accessed 24 April 2019].

[7] Y. Horbenko, "Best mHealth Apps for Patients: Doctor on Demand," [Online]. Available: https://steelkiwi.com/blog/best-mhealth-apps-for-patients-doctor-on-demand/. [Accessed 24 April 2019].

[8] E. Wicklund, "Using Apps to Bridge the Gap Between Healthcare and Health Management," 29 December 2015. [Online]. Available: https://mhealthintelligence.com/news/using-apps-to-bridge-the-gap-between-healthcare-and-health-management. [Accessed 24 April 2019].

[9] M. Jagannathan, "Mental-health apps use scientific language, but do they actually work?," MarketWatch, [Online]. Available: https://www.marketwatch.com/story/how-to-find-a-mental-health-app-that-will-actually-help-2019-03-28.

[10] Adhikari, R., Richards, D., "Security and Privacy Issues Related to the Use of Mobile Health Apps," in *25 th Australasian Conference on Information Systems*, Auckland, New Zealand, 2014.

[11] Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., Patsakis, C., "Security and privacy analysis of mobile health applications: the alarming state of practice," *IEEE Access 6,* pp. 9390-9403, 2018.

[12] S. Kumar, W. Nilsen, M. Pavel, M. Srivastava, "Mobile Health: Revolutionizing Health care Through Transdisciplinary Research," *Computer,* vol. 46, pp. 28-35, 2013.

[13] "Healthcare Data: The New Prize for Hackers," Securilink, 27 June 2018. [Online]. Available: https://www.securelink.com/blog/healthcare-data-new-prize-hackers/. [Accessed 01 Arpil 2019].

[14] A. Ng, "Your smartphones are getting more valuable for hackers," C-net, 08 March 2018. [Online]. Available: https://www.cnet.com/news/your-smartphones-are-getting-more-valuable-for-hackers/. [Accessed 01 April 2019].

[15] S. Gibbs, "WhatsApp hack: have I been affected and what should I do?," 14 May 2019. [Online]. Available: https://www.theguardian.com/technology/2019/may/14/whatsapp-hack-have-i-been-affected-and-what-should-i-do. [Accessed 14 May 2019].

[16] "Facebook's data-sharing deals exposed," 19 December 2018. [Online]. Available: https://www.bbc.com/news/technology-46618582. [Accessed 10 May 2019].

[17] "My Fitness Pal," 29 March 2019. [Online]. Available: https://content.myfitnesspal.com/security-information/notice.html. [Accessed 10 May 2019].

[18] "Security breach at MyHeritage website leaks details of over 92 million users," 6 June 2018. [Online]. Available: https://www.reuters.com/article/us-myheritage-privacy/security-breach-at-myheritage-website-leaks-details-of-over-92-million-users-idUSKCN1J1308. [Accessed 10 May 2019].

[19] Chan S., Torous, J., Hinton, l., Yellowlees P., "Towards a Framework for Evaluating Mobile Mental Health Apps," *Telemedicine and e-Health,* vol. 21, no. 12, pp. 1038-1041, 2015.

[20] O'Loughlin, K., Neary, M., Adkins, E. C., & Schueller, S. M., "Reviewing the data security and privacy policies of mobile apps for depression," *Internet interventions,* vol. 15, pp. 110-115, 2019.

[21] Braghin C., Cimato S., Libera A. Della, "Are mHealth Apps Secure? A Case Study," in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC),* 2018.

[22] P. S. Daniel J. Solove, Information Privacy Law, Wolters Kluwer Law & Business, 2015.

[23] S. Fischer-Huebner, "Privacy and security at risk in the global information society," *Information Communication & Society,* vol. 1, no. 4, p. 420–441, 1998.

[24] Rein Turn, Willis H. Ware, Privacy and security issues in information systems, Santa Monica, CA: The RAND Corporation, 1976.

[25] "Information Security and Privacy. Solutions for Data Protection and Compliance," Opentext, [Online]. Available: https://www.opentext.com/products-and-solutions/business-needs/information-governance/ensure-compliance/information-security-and-privacy. [Accessed 21 April 2019].

[26] N. Baiati, "How does GDPR impact the healthcare sector?," The Horizons Tracker, 2017. [Online]. Available: http://adigaskell.org/2017/02/04/how-does-gdpr-impact-the-healthcare-sector/. [Accessed 20 April 2019].

[27] "EU GDPR," [Online]. Available: https://eugdpr.org/. [Accessed 10 May 2019].

[28] 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, [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection_en. [Accessed 21 April 2019].

[29] "Types of EU law," European Commision, [Online]. Available: https://ec.europa.eu/info/law/law-making-process/types-eu-law_en. [Accessed 02 April 2019].

[30] "Reforming the U.S. Approach to Data Protection and Privacy," Digital and Cyberspace Policy Program, 18 January 2018. [Online]. Available: Reforming the U.S. Approach to Data Protection and Privacy. [Accessed 21 April 2019].

[31] Health Information Privacy and Portability Act of 1996 (HIPAA) Pub. L. 104 - 191, 110 Stat. 1936 (1996).

[32] United States department of Human and Health Services. Summary of the HIPAA Privacy Rule. Compliance Assistance. OCR privacy Brief HIPAA..

[33] Mobile Medical Applications. Guidance for Industry and Food and Drug Administration Staff., 9 February 2015. [Online]. Available: https://www.fda.gov. [Accessed 21 April 2019].

[34] "FDA.gov," Federal Food, Drug, and Cosmetic Act (FD&C Act), [Online]. Available: https://www.fda.gov/. [Accessed 21 April 2019].

[35] N. Beytin, "FDA takes a hands-off approach with medical mobile apps and MDDs," 13 February 2015. [Online]. Available: https://www.digitashealth.com/fda-takes-hands-approach-medical-mobile-apps-mdds/. [Accessed 21 April 2019].

[36] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993, p. 1).

[37] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices.

[38] Andrew Ruck, Susie Wagner Bondorf, Charles Lowe, "Second draft of guidelines EU guidelines on assessment of the reliability of mobile health applications. European Commission.," [Online]. Available: https://ec.europa.eu/. [Accessed 02 May 2019].

[39] "APA Privacy Policy," June 2018. [Online]. Available: https://www.apa.org/about/privacy. [Accessed 02 May 2019].

[40] M. Munz, T. Hickman, M. Goetz, "Court confirms that IP addresses are personal data in some cases," https://www.whitecase.com/publications/alert/court-confirms-ip-addresses-are-personal-data-some-cases], 2016.

[41] "Intersoft Consulting," [Online]. Available: https://gdpr-info.eu/issues/consent/.

[42] "Data Protection Commission. Anonymisation and pseudonymisation.," [Online]. Available: https://www.dataprotection.ie/en/guidance-landing/anonymisation-and-pseudonymisation. [Accessed 02 May 2019].

[43] "Anonymisation and Personal Data," Data managment guidlines, 07 October 2019. [Online]. Available: https://www.fsd.uta.fi/aineistonhallinta/en/anonymisation-and-identifiers.html. [Accessed 10 April 2019].

[44] California State Legislature. AB-375, Chau. Privacy: personal information: businesses, [Online]. Available: https://www.pbwt.com/content/uploads/2018/06/California-Consumer-Privacy-Act1.pdf. [Accessed 30 April 2019].

[45] "Guidelines on the right to data portability. Article 29 of Directive 95/46/EC Working Party," vol. 16/EN , no. WP 242 rev.01 .

[46] "Data sharing code of practice. Information Commissioner's Office," [Online]. Available: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf. [Accessed 01 May 2019].

[47] Huckvale, K., Torous, J., Larsen M. E., "Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation," *JAMA network open,* vol. 2, no. 4, pp. e192542-e192542., 2019.

[48] "What Are Cookies?," [Online]. Available: http://www.whatarecookies.com/. [Accessed 01 May 2019].

[49] S. Lele, "Cookies in Mobile: Do They Exist?," SocialMediaToday, 18 December 2014. [Online]. Available: https://www.socialmediatoday.com/content/cookies-mobile-do-they-exist. [Accessed 03 May 2019].

[50] "Cookies consent under the GDPR," EU GDPR Compliant, 14 February 2018. [Online]. Available: https://eugdprcompliant.com/cookies-consent-gdpr/]. [Accessed 02 May 2019].

[51] "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," *OJ L 201,* p. 37–47, 31.7.2002.

[52] "Encryption," Information Commissioner's Office, [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/. [Accessed 01 May 2019].

[53] T. Dierks, E. Rescorla, "The Transport Layer Security (TLS) Protocol, Version 1.2," August 2008. [Online]. Available: https://tools.ietf.org/html/rfc5246. [Accessed 1 April 2019].

[54] Rosenfeld, l., Torous, J., Vahia Ipsit V., "Data Security and Privacy in Apps for Dementia: An Analysis of Existing Privacy Policies.," *The American Journal of Geriatric Psychiatry,* vol. 25, no. 8, pp. 873-877, 2017.

[55] Mariam Bachiri, Ali Idri, José Luis Fernández-Alemán, Ambrosio Toval, "Evaluating the Privacy Policies of Mobile Personal Health Records for Pregnancy Monitoring," *Journal of medical systems,* vol. 42, no. 8, p. 144, 2018.

[56] Pietro Ferrara, Fausto Spoto, "Static Analysis for GDPR Compliance," *In ITASEC,* 2018.

[57] P. Louridas, "Static Code Analysis," *IEEE Software,* vol. 23, no. 4, pp. 58-61, 2006.

[58] "About APA," American Psychiatric Association, [Online]. Available: https://www.psychiatry.org/about-apa. [Accessed 03 March 2019].

[59] "App Evaluation Model," American Psychiatric Association, [Online]. Available: https://www.psychiatry.org/psychiatrists/practice/mental-health-apps/app-evaluation-model. [Accessed 03 March 2019].

[60] Torous, J. B., Chan, S. R., Gipson, S. Y. M. T., Kim, J. W., Nguyen, T. Q., Luo, J., & Wang, P., "A hierarchical framework for evaluation and informed decision making regarding smartphone apps for clinical care," *Psychiatric Services,,* vol. 69(5), pp. 498-500., 2018.

[61] "Why Rate Mental Health Apps?," American Psychiatric Association, [Online]. Available: https://www.psychiatry.org/psychiatrists/practice/mental-health-apps/why-rate-mental-health-apps. [Accessed 15 April 2019].

[62] "Github.com. Mobile-Security-Framework-MobSF," [Online]. Available: https://github.com/MobSF/Mobile-Security-Framework-MobSF. [Accessed 05 January 2019].

[63] J. P. Albrecht, "How the GDPR Will Change the World," *European Data Protection Law Review*, vol. 2, no. 3, pp. 287-289, 2016.

[64] "HealthIT.gov," Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA, 16 July 2016. [Online]. [Accessed 21 April 2019].