Health Apps, their Privacy Policies and the GDPR

Mulder, Trix

Published in:
European Journal of Law and Technology

Publication date:
2019

European Journal of Law and Technology, Vol 10, Issue 1, 2019

EJLT European Journal of **Law and Technology**

Health apps, their privacy policies and the GDPR

Trix Mulder[1]

Abstract

The healthcare sector traditionally processes large amounts of personal data. Nowadays, medical practice increasingly uses information technologies, such as smartphone applications ('apps') and wearable devices (e.g. smart watches, smart soles), for treatment plans and information collection. It is inherent to these modern technologies that they generate even more personal data. Some of the apps are developed specifically for the healthcare sector, some are more general (health) apps. Within the European Union (EU), the processing of these personal data is regulated by the General Data Protection Regulation (GDPR), which entered into force on 25 May 2018. The GDPR provides controllers and processors with obligations and data subjects with rights. This paper analyses the marketing statements of app providers and the privacy policies of the apps in order to determine whether they are in line with each other and with the GDPR.

1. Introduction

The healthcare industry is highly data intensive. For as long as health data has been collected, there have always been risks involved with processing this sensitive data. Accordingly, medical confidentiality prohibits a medical professional to disclose information about a patient's case. Medical confidentiality, also known as the Hippocratic Oath,[2] dates back to ancient Greece.[3] Medical confidentiality is seen as one of the most important medical paradigms because it facilitates people the seeking of medical help and being open to medical professionals.[4] However, due to modern technologies, the risks involved in processing this kind of data have changed. Examples of modern technologies are smartphone applications, wearables such as smart watches and bracelets, glasses, clothing and many more modern devices.[5] Modern technologies are increasingly used to process health data, both by healthcare professionals inside the medical context and by companies offering technologies and services to consumers outside the medical context. As a consequence, these organisations and companies have to adjust their protocols and take new technical and organisational measures to protect health data, especially in light of the new General Data Protection Regulation (GDPR).[6]

An additional complicating factor in the healthcare industry is that commercial apps and wearables are sometimes used within a medical context. However, it is not always clear how these companies who offer these technologies and services protect the health data they generate. Furthermore, as this research will show, their privacy policies do not always elucidate this either. Nowadays, digital transformation of health and care is a priority of the agenda of the EU;[7] this might be why a growing number of companies use privacy in their marketing statements.[8] This research will therefore examine to what extent differences exist between marketing statements and the actual privacy policies of apps. Secondly, it will explain the legal consequences of these differences for app companies and healthcare institutions in light of the changes brought by the GDPR. In order to do this, I will label the marketing statements of companies with regard to privacy, compare these marketing statements to their privacy policies and then link the outcome of this comparison to the GDPR in order to identify the legal consequences on a European level and determine whether the protection the GDPR offers matches with practical reality.

2. Methodology

There are more than 350,000 different apps in the category of 'health and fitness' in the three major app-stores (Apple, Google and Windows/Microsoft). Investigating all these apps would go beyond the possibilities of this explorative research. Due to the nature of this explorative research, the outcome cannot be used for statistical generalisation. The outcome is rather a theoretical observation of the use of both commercial and medical apps in medical practice.[9] Instead of randomly choosing different apps, I wanted to ensure that my research would be relevant for medical practice. Thus, I contacted three local rehabilitation centres in the Netherlands that already showed interest in my research and asked for their cooperation.[10] The rehabilitation sector is relatively broad, considering that it treats people with different medical backgrounds. It was therefore anticipated that the input for this research would lead to a broad variety of apps. Via a short questionnaire physicians were asked three questions about apps they already use, apps they want to use and apps patients suggested to use.[11] The answers contained only names of apps and or wearables and the questionnaires were treated anonymously, since it is not relevant for this research to know which physician named which app. In total, 34 different apps were mentioned by at least one physician, which were as such selected for this research.[12] In the end, two apps were no longer available and one app was only available in Belgium, which left this research with 31 apps.[13] For this research, the physicians neither shared patient information nor was this information asked for.

I divided these 31 different apps in two different categories: (1) general (health) apps and (2) apps developed for the medical sector. Apps developed for the medical sector are apps that are meant to be used inside the medical context, and thereby within a doctor-patient relationship where the medical or healthcare professional is bound by professional secrecy. General (health) apps are apps that are not developed specifically for the medical sector and some of these apps are not even developed to process health data. The intention of this article is to compare the privacy policies of the 31 apps to the provisions of the GDPR, not to name and shame the app companies. Moreover, all the privacy policies are available in the public domain. For transparency reasons the

31 apps are named in the methodology part of this research, but it is not necessary to name the apps during the analysis of their privacy policies.

There are two major legal frameworks regulating data protection in Europe: the GDPR and the Council of Europe's Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+).[14] Although Convention 108 dates back to 1982 and has a larger reach than the GDPR, considering that non-European countries can also become a State Party to the Convention, both legal frameworks follow more or less the same logic and were both updated in 2018.[15] Most of the apps selected for this research originate either from Europe or the United States (US). The US is, however, not a State Party to Convention 108. Article 3 (1) GDPR determines that the GDPR applies if the processing of personal data takes place in the context of the activities of an establishment of a controller or processor in the EU. Healthcare institutions that treat patients in Europe are most of the time established in the EU. Article 3 (2) GDPR furthermore determines that if goods or services are being offered to data subjects in the EU or if the monitoring of behaviour takes place in the EU, the GDPR applies.[16] This paper focusses on the use of apps and wearables by people in Europe. The focus of this research will consequently be on the GDPR.[17]

3. The protection of personal data

People use modern technologies for different purposes, including measuring health and fitness, keeping in touch with friends, losing weight, making photos and reducing stress. In order to use these technologies, consumers sometimes need to enter a lot of personal data. Processing personal data may lead to risks to the rights and freedoms of persons.[18] This is why the GDPR provides data subjects with rights and controllers and processors with obligations. The controller determines the purposes and means of the processing of personal data,[19] while the processor processes the personal data on behalf of the controller.[20]

Next to regular personal data, the GDPR determines that some data are more sensitive. Data concerning health is part of this special category of data. Some of the data generated by using apps may be considered data concerning health thereby enjoying stricter privacy rules given the possible impact on a person's life if this data were freely available. The GDPR, in principle, prohibits the processing of those kinds of data, unless one of the exceptions in Article 9 GDPR is met. Two of the exceptions that are relevant for this research are mentioned in Article 9 (2)(a) and (2)(h) GDPR. The first exception is when data subjects give their explicit consent to the processing, and the second exception refers to personal data that are used for medical diagnosis, the provision of healthcare or treatment of health. Article 9 (3) GDPR applies to this last exception and states that it only applies when the data are processed "by or under the responsibility of a professional subject to the obligation of professional secrecy (…) or by another person also subject to an obligation of secrecy…". In the Netherlands, the Civil Code regulates professional secrecy for healthcare professionals.[21]

When data concerning health are processed by commercial parties via their apps and wearables, it

is clear from the provisions of the GDPR that the data subject's explicit consent is needed, otherwise processing is prohibited.[22] Therefore, this paper examines whether requesting consent is compliant with the GDPR. Article 6, 7 and 9 (2)(a) GDPR are the relevant articles relating to consent of the data subject. Since these apps collect the personal data from the data subject, Articles 12 and 13 GDPR are also of importance. Article 13 gives an overview of the information the controller needs to provide to the data subject, and Article 12 determines that this information needs to be provided "in a concise, transparent, intelligible and easily accessible form, using clear and plain language". The privacy policies of these apps were examined to determine whether the app companies or healthcare institutions comply with the GDPR. Finally, the principles relating to processing of personal data of Article 5 GDPR will be used to determine whether the privacy polices comply with the GDPR.

As regards the processing of data concerning health within the medical context, the data subject's consent is not needed since the exception of Article 9 (2)(h), in conjunction with (3), applies. However, in that case, the processing has to take place 'under responsibility' of a physician. When commercial apps and wearables are used in a medical context, it must be questioned whether this requirement is met, considering that the data are stored on the device of the patient, i.e. on their smartphone, or on the servers of the app provider. Furthermore, it is the app that determines exactly what data are collected, meaning that there is possibly more data processed then necessary for treatment of the patient. The GDPR does not explain what is meant by 'under responsibility', and the preamble does not elaborate on this further. This research therefore presumes that data processing of commercial apps used in a medical context does not take place 'under responsibility' of the physician. This means that explicit consent of the data subject is required. Since this research focusses on the use of apps and wearables by adults, the specific provisions on consent of children below the age of 16 will not be discussed.

Finally, there are apps that are developed specifically for the healthcare sector. According to Directive 2007/47/EC these apps are medical devices.[23] For these apps, the data will be processed under responsibility of the physician, and thus consent is not needed. However, these apps still have to meet the requirements of Article 12, in conjunction with Article 13, GDPR. Therefore, this research will analyse these apps to find out whether this is the case in practice. However, before moving on to the analysis of the privacy policies in section 4, the next section will first discuss the marketing statements of the app companies which were selected for this research. For this research, the public websites of the app companies where investigated to see if they contained any general remarks relating to privacy.

4. Marketing statements

Research has shown that marketing statements are an important tool for companies and they encourage people to buy goods and transact services.[24] This raises the question whether people give their consent to the text in the privacy policies, or if they rely on marketing statements rather than reading the privacy policies themselves, especially since research has shown that most of the

people never read privacy policies.[25] Most people formally consent to privacy policies without knowing what happens to their personal data. This does not automatically make the processing lawful. However, it is the question whether actually reading a privacy policy will help to understand what is happening to the personal data. The analysis of the privacy policies will be discussed in the next section. This section will first evaluate the marketing statements by the companies of the selected apps.

4.1 General (health) apps

Online research into the selected apps, showed varying approaches as regards privacy. Most of the apps - nine in total (see table 1) - mentioned privacy in their marketing statements, demonstrating a positive attitude towards privacy. These statements are not part of the company's privacy policy; rather, they are stand-alone marketing statements, ranging from "Some of your most personal moments are shared (…), which is why we built end-to-end encryption (…) your messages and calls are secured so only you and the person you're communicating with can read or listen to them, and nobody in between…"[26] to "(Our) products are designed to do amazing things. And designed to protect your privacy. (…) we believe privacy is a fundamental human right."[27]

Alongside the nine companies that use privacy in their marketing statements, there are seven companies that do not really use privacy as a marketing statement. Notably, they start their privacy policies by emphasising that privacy is important to the company. One could see this as a marketing statement in disguise, especially since all seven companies use such sentences in the beginning of their respective privacy policy. It could lead the reader to believe that, since the company emphasises on how important privacy is to them, the companies are careful in handling the user's personal data.

Finally, there are seven other app companies that do not mention anything on privacy at all and their privacy policies are a more formal representation on how they handle their users' privacy. The tone of these policies is very different from the other seven companies that seem to use the beginning of their privacy policy as a marketing statement. Those first seven companies use phrases such as "Your privacy is important to (us)…"[28] and "(We) respect your privacy and share your concern about the security of information you may submit to (us)."[29] The other seven companies, which use more formal representation, start their privacy policies with sentences such as "This privacy policy describes the personal data collected or generated (processed) when you use (…) our mobile applications"[30] and "To provide our products, we must process information about you. The types of information we collect depend on how you use our Products."[31]

	Marketing statement	Use of marketing via privacy policy	No marketing statement
General (health) apps	9 (6)*	7	7

Table 1: use of privacy as a marketing statement by general (health) apps

* These nine apps are developed by six different companies; therefore, some marketing statements were used twice or thrice.

Thus, the selected apps that are not specifically developed for the medical sector show a scattered

image when it comes to using privacy as a marketing statement. The next section will investigate if the same can be said for apps that are developed for the medical sector.

4.2 Apps developed for the medical sector

This research analysed eight apps that are specifically developed for the medical sector which are still available. It turned out that four of those apps are only available on a tablet, not on a mobile phone or wearable. Online research of the companies that offer the apps shows that none of these companies use privacy as a marketing tool. Surprisingly enough, only one of the eight apps has a separate privacy policy that they offer to the user before the download or use of the app. This company uses a formal tone in its privacy policy and makes no real marketing statements within it. Three out of the other seven apps are paid apps, and there is no available information as to how they deal with privacy, at least not before payment. Finally, one app mentions how they deal with privacy in their general terms and conditions, which the user can open before logging in and using the app. The other three apps do not mention privacy at all.

	Marketing statement	Use of marketing via privacy policy	No marketing statement
Apps for the medical sector	0	0	8

Table 2: use of privacy as a marketing statement by apps developed for the medical sector

As far as marketing statements are concerned, the apps developed for the medical sector show a more uniform picture; none of the analysed apps use privacy as a marketing tool. The question whether not having a separate privacy policy is in accordance with the GDPR will be discussed in the next section.

5. Privacy policies

Processing of personal data can only be lawful if one of the conditions of Article 6 GDPR is met. One of the conditions is consent given by the data subject.[32] As mentioned in section 2, consent is the most common basis for lawful processing when it comes to processing data concerning health via apps. Before analysing the privacy policies, this section first discusses the legal concept of consent.

5.1 Consent

Consent in the GDPR is defined as "…any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[33] This is

why the term 'informed consent' is often used. Consent is informed when the data subject is aware of the identity of the controller and the purposes of the processing for which the personal data are intended.[34] How consent has to be given is not determined by the GDPR, meaning that it is free form and can be given via a written declaration or an oral statement.[35] However, Article 7 GDPR determines that the controller needs to be able to demonstrate that the data subject has given his or her consent.[36] As a consequence, a written statement, such as an 'I-agree-button' combined with a privacy policy, is one of the most common mechanisms to comply with Article 7 GDPR.

Data concerning health are considered to be sensitive data. Processing of this type of data is, in principle, prohibited by the GDPR.[37] Sensitive data can only be processed if one of the requirements in Article 9 (2) GDPR is met. Consent by the data subjects is, again, one of the exceptions. However, the GDPR does not stipulate regular informed consent in this case, but rather explicit consent. Unfortunately, neither the GDPR nor the preamble of the GDPR defines what is meant by explicit consent; one can therefore only assume that the bar is set higher than for informed consent. According to the Article 29 Working Party,[38] the term 'explicit' refers to "…the way consent is expressed by the data subject."[39] They illustrate this by giving an example: a written statement from the data subject, preferably signed, is considered to be explicit. In a digital online context, there are also other ways to give explicit consent, such as via an electronic form, an email, a scanned document with the signature of the data subject and an electronic signature.[40]

Whether consent is explicit or not, Article 7 GDPR applies. This article determines that the controller needs to be able to demonstrate that consent was given, but also determines that the request for consent needs to be presented in a way that is clearly distinguishable from other matters.[41] This means that, if a written declaration also concerns other matters, consent needs to be clearly distinguishable within this written declaration. Furthermore, consent has to be offered to the data subject in an intelligible and easily accessible form, using clear and plain language. The latter means that an average person should be able to understand the request for consent. Therefore, the text must not be too long, difficult to understand or full of legal jargon.[42] If these demands are not met, consent is not binding.[43] Additionally, data subjects should be informed, before giving consent, that they have the right to withdraw their consent at any time.[44]

5.1.1 Privacy policies and consent

18 of the analysed apps use consent as a legal basis for processing personal data and thus need to comply with Article 7 (2) GDPR. To measure the obligation laid down in that article, it is divided into two parts. Since this research focuses on written privacy policies, it was first necessary to verify whether the request for consent was presented in a manner which is clearly distinguishable from other matters. That was the case for all the 18 apps, as they did not use other documents, such as general terms and conditions, to request consent. All of them asked for consent in a separate pop-up and had a separate privacy policy.

	Consent as a legal basis (written declaration)	Article 7 (2) GDPR: presented in a manner which is clearly distinguishable from other matters	Article 7 (2) GDPR: intelligible and easily accessible form, using clear and plain language
Analysed apps (31)	18	18	18

Table 3: Requirements for consent (Article 7 (2) GDPR).

Article 7 (2) GDPR also determines that the text needs to be available in an intelligible and easily accessible form, using clear and plain language. It is not easy to measure whether the used language is clear and plain. According to the Article 29 Working Party, clear and plain language means that "a message should be easily understandable for the average person and not only for lawyers."[45] As regards the request for consent by and even the privacy policies of the 18 analysed apps, the language was easily understandable and no legal jargon was used. This is thus in compliance with the GDPR. However, none of the apps, not even the general health apps, met the conditions set by the Article 29 Working Party on explicit consent. Furthermore, the privacy policies had difficulties complying with the conditions of Article 12 in conjunction with Article 13 GDPR.

5.2 Article 13 GDPR

Article 13 GDPR deals with the information the controller needs to provide the data subject with at the time the personal data are obtained from the data subject. This article has to be read in conjunction with Article 12 GDPR, which determines that the controller has to provide the information in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This section will be divided according to the provisions of Article 12 and 13 GDPR.

5.2.1 Information to be given by the controller

Article 13 GDPR determines that the controller has to inform data subjects about, for example, their rights, the purpose(s) for processing and the recipients or categories of recipients, in line with the conditions of Article 12. This has to be done in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Although it is difficult to measure whether the privacy policies meet these requirements, one thing that stands out immediately is the length of the privacy policies. On average, the analysed privacy policies consist of 3,783 words; the largest had 11,344 words and the smallest 347 words. Knowing that a person reads 200 – 250 words per minute, this means that it will take, on average, approximately 15 – 20 minutes to read these policies. Only four privacy policies used less than 2,000 words.

	Separate privacy policy	< 2.000 words

Privacy policies analysed apps (31 apps in total)	20 (17 different policies)	4 (on average 3.783 words)

Table 4: Separate privacy policies and word count.

An analysis of Article 13 (1) and (2) GDPR leads to 18 different conditions the data controller needs to meet.[46] Of the four apps with less than 2,000 words, three apps only met either six or eight out of the 18 conditions in Article 13 GDPR. However, one of these four apps had a privacy policy of 1,152 words and was still able to meet 14 out of the 18 conditions in Article 13.

Furthermore, three apps had the same privacy policy as they were from the same app developer. As a result, the following table only shows 17 apps. What is striking is that none of the apps that had a privacy policy complied with all 18 conditions (see table 5). One must question why this is the case..

	Compliant to Article 13 GDPR (18 provisions)	Compliant to Article 12 GDPR
App 1	13 (18)	No
App 2	13 (18)	No
App 3	6 (18)	No
App 4	13 (18)	No
App 5	9 (18)	No
App 6	14 (18)	No
App 7	12 (18)	No
App 8	11 (18)	No
App 9	13 (18)	No
App 10	8 (18)	No
App 11	9 (18)	No
App 12	6 (18)	No
App 13	14 (18)	No
App 14	14 (18)	No
App 15	15 (18)	No
App 16	14 (18)	No
App 17	12 (18)	No

Table 5: Apps with a privacy policies and Article 13 GDPR.

Two things can be noticed. Firstly, only one of the analysed privacy policies complies with the conditions of Article 12 GDPR. Secondly, only two privacy policies meet the conditions set in Article 13 (1) (c), in conjunction with Article 5 (1)(b), GDPR, which determines that the data subject needs to be informed about the purposes for processing and that data can only be collected for specified, explicit and legitimate purposes.

Article 12 uses some terms that can be considered subjective. For instance, with regards to concise information, the question arises as to what exactly is meant by transparent information and clear and plain language.[47] The Article 29 Working Party does not mention when information is concise and transparent. Therefore, this research analysed those terms and investigated how many times the word 'may' was used in combination with 'we' in order to get a picture of how companies use the personal data. The research further monitored how many times the words 'include' and/or 'including' were used in combination with the data the companies collect. Without purporting to be complete, these two combinations of words give an idea of how concise the provided information is.

While reading and analysing the privacy policies, one notices that it is difficult, if not impossible, to get a complete picture of what the app providers do with the personal data they collect. The language that these companies use is vague and leaves the reader with many questions, such as statements that they "collect personal data", "may share data" or "may collect the following information about you." The use of this kind of language is not rare; all but one of the app providers used this kind of language at least 20 times and in some cases even more than 50 times. As a result, it is difficult to get a complete overview of what is being done with the collected personal data. In only two out of the 18 apps, there was the possibility to match the collected personal data to the purposes for processing. If it is not clear what the purposes for the processing exactly are, the conclusion has to be that consent is not informed, and, therefore, the processing unlawful.

Article 13 (1)(c) GDPR determines that the purposes for processing for which the personal data are intended need to be provided by the controller. When reading the privacy policies, it was very difficult to find out the purposes of collecting different types of data. All analysed privacy policies provided purposes for processing. The clarity of these purposes varied from very vague "We use (your personal data) to improve our (…) services"[48] to more concise "We use the information we have about you (…) to select and personalise ads…".[49] Not one policy was clear about the correlation of the collected data and the purposes for which they are collected. This is surprising, considering that Article 5 (1) (b) GDPR determines that personal data can only be collected for specified, explicit and legitimate purposes. The GDPR makes organisations and companies evaluate their processes and be transparent about this. It is therefore necessary that app providers clearly formulate their specified and explicit purposes for processing, meaning they have that information, so why not inform the data subject about it?

5.2.2 Other provisions of Article 13 GDPR

According to Article 13 GDPR, the controller needs to provide the data subject with information at the time when the personal data are obtained from the data subject.[50] This information could therefore be provided simultaneously with downloading the app, depending on when the data collection starts. However, if the app registers which accounts download the app, data subjects need to be informed as soon as downloading starts, considering that account registration is already processing of personal data.

No privacy policy of apps developed for the medical sector

Apps that are specifically developed for the medical sector almost certainly process personal data that are considered to be data concerning health. Considering that these apps are specifically developed for the medical sector, we can assume that the data processed by these apps are processed either by or under the responsibility of the physician who has the obligation of professional secrecy. As a consequence, Article 9 (2) (h) in conjunction with Article 9 (3) GDPR applies, meaning that explicit consent of the data subject, i.e. the patient, is not needed. This also means that Article 7 GDPR, which sets conditions for consent, does not apply. However, the provisions of Article 12 in conjunction with Article 13 GDPR do apply.

Out of the eight apps developed for the medical sector analysed for this research, only one app had a privacy policy. However, a privacy policy is not the only way to comply with Article 12 in conjunction with Article 13 GDPR, particularly considering that, in this case, the GDPR does not require the controller to demonstrate that the information was provided to the data subject. In such cases, it would thus be sufficient for the physician to provide the patient with the information orally or, for example, by providing a hand-out. One would expect this to be general practice, considering that almost none of these apps had a separate privacy policy. However, there is still the question of whether, in that case, the information is as complete as it needs to be. After all, a physician is not a technician nor a lawyer. So, would the physician be the best person to provide this kind of information to the patient?[51]

Commercial apps without privacy policies

With regard to commercial (health) apps that physicians use or would like to use for the treatment of their patients, this research analysed 23 apps. 19 out of 23 apps had a separate privacy policy. 4 out of 23 apps did not have a privacy policy at all, and two did not even mention privacy. Further investigation (downloading and using the apps) showed that these two apps do not need to process personal data in order to function. Considering that these apps can function without personal data and that there is no information provided under Article 13 GDPR, one might assume that these apps do not process personal data. The question remains whether this is the case, since personal data is a very broad concept. As stated above, if the app registers which accounts download the app, they process personal data and therefore have to provide the information under Article 13 GDPR.

One of the apps that did not have a privacy policy had a link to a privacy policy which did not function. It furthermore notifies data subjects as soon as the app is downloaded that they comply with applicable legislation, without elaborating on what the applicable legislation is. If the app does not process personal data, this is not a problem. However, the app does process personal data, considering that it mentions that all processed information stays on 'your' device. The app is designed to calculate a person's contribution to healthcare costs which is considered to be personal data.[52] The other app that did not have a privacy policy also mentions that all the information stays on the device. The purpose of that app is to make people aware of the importance of relaxation and offers exercises to improve relaxation. This data can also be considered personal data, as soon as it can be linked to a natural person. In both cases, the app

providers are the controllers, since they determine purpose and means for the processing.[53] It is therefore not relevant whether the personal data are processed on the device or are transferred to a server of the app provider, considering that Article 13 GDPR requires the controller to provide the data subject with information. These two apps do not provide data subjects with information via a privacy policy or in any other way, before or right after downloading the app, and are thus in violation of Article 13 GDPR.

	No processing of personal data necessary, and therefore no violation of Article 13 GDPR*	Personal data processed, therefore violation of Article 13 GDPR
No privacy policy	2	2

Table 6: processing of personal data without a privacy policy

* Since processing of personal data is not necessary for the apps to function, the assumption is made that no personal data are being processed. If this is the case, they also act in violation with Article 13 GDPR.

Commercial apps with privacy policies

According to Article 13 (1)(a) and (b) GDPR data subjects need to be informed of the identity and contact details of the controller and of the contact details of the data protection officer (DPO). Out of the 19 apps that did have a privacy policy, almost all provided this information; all apps provided the contact details of their DPO, if they had one, and 16 apps provided the identity and contact details of the controller.[54]

	Article 13 (1)(a) GDPR (identity and contact details controller)	Article 13 (1)(b) GDPR (contact details DPO)
Compliant apps	16	19

Table 7: provisions of Article 13 (1) (a) and (b) GDPR.

The same can be said as regards the requirement to inform data subjects of their rights. In particular, the right of access, the right to rectification and the right to erasure are mentioned in almost all privacy policies. One privacy policy does not mention the rights of data subjects at all, and one mentions the rights of data subjects, but fails to explain how these rights can be exercised.

	Art. 13 (2)(b) GDPR (existence right to request access)	Art. 13 (2)(b) GDPR (existence right to request rectification)	Art. 13 (2)(b) GDPR (existence right to request erasure)	Art. 13 (2,c) GDPR (right to withdraw consent at any time, without affecting lawfulness of processing before)	Art. 13 (2)(b) GDPR (existence right to request restriction of processing)	Art. 13 (2)(b) GDPR (existence right object to processing)	Art. 13 (2)(b) GDPR (right data portability)	Art. 13 (2)(d) GDPR (right to lodge complaint with supervisory authority)
Compliant apps	18	18	18	15	14	13	15	13

Table 8: provisions of Article 13 (2)(b) and (c) GDPR.

As regards the right to withdraw consent at any time, four out of 19 apps do not mention this right, while they do process personal data based on consent. Two out of the four apps that do not mention the right to withdraw consent also do not mention the right data portability. These are the same two apps that also do not mention other rights, especially the right to restriction of processing, the right to object and the right to lodge a complaint with the supervisory authority.

Both the right to lodge a complaint with the supervisory authority and the right to object to the processing[55] are less provided for than the other rights; however, a majority of two-thirds of the apps do provide data subjects with this information.

	Art. 13 (1)(c) GDPR (purposes for processing (collected for specified, explicit and legitimate purposes, art. 5 (1) (b) GDPR)	Art. 13 (1)(c) GDPR (legal basis for processing)	Art. 13 (1((e) GDPR (recipients or categories of recipients)	Art. 13 (1)(f) GDPR (transfer to 3rd country: existence or absence adequacy decision or reference to appropriate safeguards and means to obtain a copy)	Art. 13 (2)(a) GDPR (period personal data will be stored, or criteria to determine that period)
Compliant apps	2	0	1 / 19	3	3

Table 9: provisions of Article 13 (1) (c), (e) and (f) and (2) (a) GDPR.

With regards to the legal basis for processing, none of the apps link all the legal bases for processing with the collected data. The GDPR furthermore determines that data subjects have to be informed about the recipients or categories of recipients. Only one app states that there are no recipients. The other 18 apps only mention categories of recipients, such as corporate affiliates, service providers, and other partners or subsidiaries and controlled affiliates located in the U.S. or elsewhere, as we believe necessary for business purposes. These categories are very broad. It is, for example, not clear who these 'other partners' are, how many 'other partners' there are and if these 'other partners' often change. Therefore, it is nearly impossible for data subjects to determine where and how their personal data flows.

Article 13 (1) (f) GDPR determines that if the controller intends to transfer personal data to a third country, the data subject needs to be informed of the existence or absence of an adequacy

decision by the Commission. If such an adequacy decision does not exist, a reference has to be made to the appropriate or suitable safeguards. Only three privacy policies comply with this rule. Apps which are covered by the EU – US Privacy Shield Framework mention this. Some app providers mention the Privacy Shield Framework as an example, although they are not a member themselves. Other app providers mention that they are "required by applicable law, (to) ensure that your privacy rights are adequately protected by appropriate technical, organisation, contractual or other lawful means." They fail to explain how this is done. Some even mention that they transfer data to third countries, "some of which have not yet been determined by the European Commission to have an adequate level of data protection." Considering the aforementioned, this cannot be seen as a reference to appropriate or suitable safeguards.[56] This means that the processing of these data is unlawful.

It can therefore be concluded that while some of the provisions of Article 13 GDPR are covered relatively well by the privacy policies, other provisions are covered poorly. The requirements that were least met include the purposes and legal bases for processing in combination with the personal data that are processed, the recipients of the data and the transfer of data to a third country. Although it is encouraging that most of the app providers inform data subjects of their rights, it is worrying that it is almost impossible for data subjects to find out where in the world their data are processed and what are the exact purposes for processing. This, in turn, makes the processing of these data unlawful. Here lies the role of the supervisory authorities to enforce the provisions of the GDPR. If healthcare institutions want to use these apps, they have to be more active and stimulate app companies to be more open on these key elements of data protection.

6. Discussion

In comparing the privacy policies of companies to the provisions of the GDPR, some results were surprising. Almost 50% of the analysed apps used privacy as a positive marketing statement. This is sometimes done on the website of the app provider and sometimes via the first lines of the privacy policies. All these statements give the reader the impression that the company believes their clients' privacy is important. However, reading the entire privacy policies shows that the policies do not actually merit that impression. In particular, when it comes to the purposes of processing personal data, the policies remain vague. Out of the 18 apps that used consent as a legal basis for processing, there were only two for which it was possible to match the collected personal data to the purposes for processing via the privacy policies. This is especially strange, as the GDPR determines that controllers and processors can only process personal data for specified, explicit and legitimate purposes. Since the companies therefore have this information, they can share it with data subjects. However, this is not the case, which leads to the question of why companies do not share this information. Besides, in some of the cases, the processing of personal can even be considered to be unlawful. The situations this research encountered as such are when (1) the purposes for processing are not clear (Article 13 (1)(c) GDPR), (2) it is not clear where in the world the data are being processed and (3) the reference to appropriate or suitable safeguards is missing (Article 13 (1)(f) GDPR).[57]

The section on the marketing statements made it clear that 16 apps used privacy in their marketing statements or used the first phrases of their privacy policies to state that they believe the data subject's privacy is important. Out of these 16 companies, seven companies did not use marketing statements in general, but used the first phrases of their privacy policy to emphasise how important they believe their user's privacy to be. Remarkably, two out of these 16 apps did not have a privacy policy at all. The other 14 apps met at least ten of the 19 analysed requirements of the GDPR.

	Privacy as marketing	No privacy policy	Requirements Article 13 GDPR
Companies	16	2	> 10 of 19

Table 10: Combining marketing statement with privacy policies.

Two out of 16 app providers used privacy as a marketing statement, without having a separate privacy policy, while four app providers that did not use privacy in their marketing statements did have a privacy policy. Interestingly enough, most of the app providers claim that they believe data subjects' privacy is important even though this is not reflected in their privacy policies.

Another element is that out of the eight analysed apps that were developed specifically for the medical sector, only one had a privacy policy. Those apps do not process the sensitive personal data on the legal basis of explicit consent; they process the personal data on the exception of Article 9 (1)(h) in conjunction with Article 9 (3) GDPR, considering that those data are processes under the responsibility of a physician with professional secrecy. Even though Article 7 GDPR does not apply in that case, the information of Article 13 GDPR still has to be provided for. The question remains this information can and would be provided for by physicians. Can we expect physicians to be able to explain every element of Article 13 GDPR to their patients? This is not necessary, especially since there are other means by which the information can be provided, for example via a privacy policy.

Since the healthcare sector and physicians feel the need to increasingly use commercial apps for treatment purposes, they need to improve their involvement. Given that the privacy policies of companies are vague regarding some key elements of data protection, the healthcare sector and physicians need to indicate what is important for them before they can start using the commercial apps in their medical practice. The healthcare sector and physicians have to comply with more rules than just data protection, with medical confidentiality being one of those rules. [58] Since the healthcare sector almost always processes sensitive personal data on a large scale, this gives them a special status which also leads to responsibilities. Albeit, it is not possible for an individual physician to gain a complete overview of all the legal and non-legal frameworks that apply to them. In addition, there is the question of whether an individual physician has time to make such an overview. Furthermore, their individual scope of influence will probably not be significant enough. This therefore means that the healthcare sector, on a national or even European level, should work together to enlarge their scope of influence and to be able to determine their set of

rules.

This article showed that, in some cases, the current privacy policies that companies use do not comply with the provisions of the GDPR. Even if the healthcare sector is able to unite and finds ways, together with the app companies, to improve the current situation regarding privacy policies, there is still the issue of people not reading these privacy policies. There are several possible solutions that could improve the challenge concerning informed consent. Firstly, personalised privacy policies might persuade people to read the privacy policy that is presented to them.[59] Secondly, privacy policies could be written for smart machines instead of people. That way, consent could be delegated to these smart machines on the basis of one's preference.[60] An alternative solution is to use icons to explain the possible impact on a person's privacy to people,[61] and finally people could be nudged into reading privacy policies.[62] Although further research has to be done regarding the pros and cons of these solutions, it does show that informed consent might still be a way to empower people in the near future.

7. Conclusion

The GDPR became binding law on 25 May 2018 and all of the privacy policies that were outdated,[63] were adjusted in April or May 2018. Presumably, this has something to do with the GDPR; however, considering that the older versions of the policies were not analysed, this cannot be said with absolute certainty. What can be said is that all privacy policies more or less comply with some of the provisions of the GDPR, especially the provisions on providing data subjects with information, in particular the identity and contact detail of the controller and the rights of data subjects. However, being open as regards the collected data and the purposes of this data collection, as well as being concise and transparent is not reflected in the privacy policies.

While marketing statements lead you to believe that 'your' privacy is important, this is not reflected in companies' privacy policies. Being transparent about processing activities, including what data is collected for which purposes, is necessary to help data subjects understand what really happens with their data. There are very easy ways to be transparent, for example, by including an information table to link the collected personal data to the purposes and legal bases for processing. This is not only important for data subjects, but also for healthcare professionals in their decision on whether or not to use commercial apps in their practice.

Considering the companies' marketing statements, as well as the need for using commercial apps in medical practice, it would be advisable for supervisory authorities or the European Data Protection Board (EDPB) to discuss this subject with representatives of both sectors. The healthcare sector not only needs to comply with data protection rules but also to, for example, medical confidentiality. It is therefore key to discuss their needs with app providers before use of the apps for treatment purposes. Traditionally, the healthcare sector works closely with the pharmaceutical industry as regards prescription of drugs for treatment of patients. This collaboration can also be very useful when it comes to app providers.

A cooperation between the EDPB and representatives of app providers and the healthcare sector on this matter is desirable, considering that together they can create solutions which benefit all,

including data subjects. This will make it easier for all app providers to comply with the GDPR, including particular needs of the healthcare sector, and for national supervisory authorities to enforce these regulations.

---

[1] Trix Mulder LLM, PhD Candidate at the Security, Technology and e-Privacy research group at the Faculty of Law at the University of Groningen.

[2] The classic version Hippocratic Oath dates back to approximately 400 B.C. and the translation by Ludwig Edelstein in 1943 reads 'What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about.'

Edelstein, L (1943), The Hippocratic Oath: Text, Translation, and Interpretation (Baltimore: Johns Hopkins Press).

[3] Weichert, T, ABIDA report 'Big Data im Gesundheitsbereich', 01IS15016A-F, via: <http://www.abida.de/sites/default/files/ABIDA%20Gutachten-Gesundheitsbereich.pdf> p. 10, accessed 17 December 2018.

[4] Munss, C and Basu, S (2016), Privacy and healthcare data: 'Choice of Control' tot 'Choice' and 'Control' (Routledge).

[5] For example: <https://ec.europa.eu/digital-single-market/en/news/mirror-mirror-wall-who-healthiest-them-all> and <https://ec.europa.eu/digital-single-market/en/news/do-you-drink-enough-ask-your-shirt-do-you-eat-too-much-ask-your-glasses>, accessed 17 December 2018.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), article 5 paragraph 1 sub a. The GDPR goes into effect May 2018.

[7] See for example the rapport on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, Brussels COM(2018) 233 final.

[8] The term 'marketing statement' is most of the time part of a company's mission statement and/or business model. However, for this research the term marketing statement is interpreted as an expression of a company on their public website with regard to privacy.

[9] Yin, R (2014), Case Study Research, Design and Methods (Sage Publications: Thousand Oaks).

[10] Beatrixoord, Roessingh and De Hoogstraat.

[11] The questions were: **1.** Do patients ever suggest using an app or wearable in their rehabilitation process that they already use or would like to use and, if so, which apps and wearables are this and where do they want to use them for? **2.** Have you ever advised an app or wearable yourself and, if so, what apps or wearable and for what part of the rehabilitation process?; **3.** Are there apps or wearables that you have not yet advised, but would like to advise and if so what would that app or wearable be suitable for?;

One of the revalidation centres conducted a similar inquiry themselves a few weeks earlier, therefore the data of those questionnaires where used instead of the questions above.

[12] For this research I did not have access to any patient data or other personal data of the physicians that participated in the research. Before I started my PhD the Committee for Academic Practice from the Faculty of Law approved my proposal, this research was part of that proposal.

[13] The apps are: (Apps for the medical sector) Activiteitenweger jongeren, Oefen App Beroerte, TIAS-app, Beenamputatie en prothese, Finger Motion, Pictoplanner, Gespreksboek app, Communicado, Mindfulness app VGZ, (general health apps) Versterk je enkel, EB app WMO, Fitbit, VidyoMobile, Nike running, Strava, Calm (general apps)

Dexteria Dots 2 , Ubersense coach, Notitie App, Google Maps, Skype, Any.do, 3D-brain, Color Note, Google Calendar, Facebook messenger, Facetime, Google documents, Whatsapp, Photogrid, 9292.

[14] Convention for the protection of individuals with regard to automatic processing of personal data [1981] ETS No. 108 (CM/Inf(2018)15-final).

[15] Although the General Data Protection Regulation already entered into force in 2016 it only became applicable as of 25 May 2018 (Article 99 (2) GDPR).

[16] Article 3 GDPR.

[17] The US have an observer status and although they signed six treaties Convention 108 is not one of them, see: < https://www.coe.int/en/web/conventions/search-on-states/-/conventions/treaty/country/USA>, accessed 17 December 2018.

[18] Recital 2 GDPR.

[19] Article 4 (7) GDPR.

[20] Article 4 (8) GDPR.

[21] Article 457 of Book 7 Dutch Civil Code.

[22] Article 9 (1) GDPR.

[23] A medical device is "any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, together with any accessories, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of:
- diagnosis, prevention, monitoring, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,
- investigation, replacement or modification of the anatomy or of a physiological process,
- control of conception, and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means;'
OJ L 247, 5.9.2007, p. 21 states: "It is necessary to clarify that software in its own right, when specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device, is a medical device. Software for general purposes when used in a healthcare setting is not a medical device."

[24] See for example: Hoffman, D (2006), 'The Best Puffery Article Ever', Iowa Law Review 91, available at SSRN <https://ssrn.com/abstract=887720>, accessed 17 December 2018; Morasch, M (2004), Comparative Advertising - a Comparative Study of Trade-Mark Laws and Competition Laws in Canada and the European Union (University of Toronto, Faculty of Law), available at SSRN <https://ssrn.com/abstract=685602> accessed 17 December 2018.

[25] McDonald, A and Cranor, L (2008), 'The Cost of Reading Privacy Policies', A Journal of Law and Policy for the Information Society; Schaub, F Balebako. R and Cranor, L (2017) 'Designing Effective Privacy Notices and Controls', IEEE Internet Computing 99.

[26] Marketing statement app 32, accessed 30 August 2018.

[27] Marketing statement app 19, accessed 30 August 2018.

[28] Privacy policy app 18, app 19 and app 24.

[29] Privacy policy app 21.

[30] Privacy policy app 20.

[31] Privacy policy app 29.

[32] Article 6 (1,a) GDPR.

[33] Article 4 (11) GDPR.

[34] Recital 42 GDPR.

[35] Recital 32 GDPR.

[36] Article 7 GDPR.

[37] Article 9 (1) GDPR.

[38] With the entry into force of the GDPR the Article 29 Working Party became the European Data Protection Board (EDPB); see Article 68 GDPR.

[39] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259rev.01, 10 April 2018, p. 18.

[40] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259rev.01, 10 April 2018, p. 18..

[41] Article 7 (2) GDPR.

[42] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259rev.01, 10 April 2018, p. 14.

[43] Article 7 (2, final sentence) GDPR.

[44] Article 7 (3) GDPR.

[45] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP250rev.01, 10 April 2018, p. 14.

[46] This research analysed the following 18 provisions: (1) Art. 13 (1,a) GDPR: identity and contact details controller; (2) Art. 13 (1,b) GDPR: contact details dpo; (3) Art. 13 (1,c) in conjunction with art. 5 (1,b) GDPR: purposes for processing, collected for specified, explicit and legitimate purposes; (4) Art. 13 (1,c) GDPR: legal basis for processing; (5) Art. 13 (1,e) GDPR: recipients or categories of recipients; (6) Art. 13 (1,f) GDPR: transfer to 3rd country, existence or absence adequacy decision or reference to appropriate safeguards and means to obtain a copy; (7) Art. 13 (2,a) GDPR: period personal data will be stored, or criteria to determine that period; (8) Art. 13 (2,b) GDPR: existence right to request access; (9) Art. 13 (2,b) GDPR: existence right to request rectification; (10) Art. 13 (2,b) GDPR: existence right to request erasure; (11) Art. 13 (2,b) GDPR: existence right to request restriction of processing; (12) Art. 13 (2,b) GDPR: existence right object to processing; (13) Art. 13 (2,b) GDPR: right to data portability; (14) Art. 13 (2,c) GDPR: right to withdraw consent at any time, without affecting lawfulness of processing before; (15) Art. 13 (2,d) GDPR: right to lodge complaint with supervisory authority; (16) Art. 13 (2,e) GDPR: if provision of personal data is obliged to provide the personal data for the contract and the consequences of failure to provide such data; (17) Art. 13 (2,f) GDPR: existence of automated decision making, including profiling and if that is the case, meaningful info about the logic involved and (18) Art. 13 (2,f) GDPR: for further processing for another purpose, prior to further processing.

[47] As seen in paragraph 4.1.1, the Article 29 Working party mentioned that clear and plain language means that the message should be easily understandable for the average person.

[48] Privacy policy app 25.

[49] Privacy policy app 29.

[50] See also recital 61 GDPR.

[51] It was not within remit of this research to examine how the information is provided in practise.

[52] See Article 4 (1) GDPR for the definition of personal data: “any information relating to an identified or identifiable natural person”.

[53] After all, the app provider chooses the app (means) and the purpose (relaxation, calculations, etc.).

[54] Some apps only provided an email address as contact detail, but since the GDPR does not determine what contact details have to be provided, this is considered to be enough to be compliant.

[55] Article 13 paragraph 2 (b) GDPR.

[56] Simply mentioning that personal data is transferred is not enough. After all, Article 13 (1)(f) GDPR determines that a reference has to be made to appropriate or suitable safeguards.

[57] These examples are discussed in section section 5.2.1 of this research.

[58] For example: Jenkins, G Merz J and Sankar, P (2005) 'A qualitative study of women's views on medical confidentiality', Journal of Medical Ethics 31; Appari, A and Johnson, M (2010) 'Information security and privacy in healthcare current state of research', International Journal Internet and Enterprise Management 6.

[59] On personlised law see for example: Busch, C (2018) 'Implementing Personalized Law: Personalized Disclosures in Consumer Law and Privacy Law', University of Chicago Law Review forthcoming, available at SSRN <https://ssrn.com/abstract=3181913>, accessed 17 December 2018.

[60] For example: Busch, C (2018), 'Implementing Personalized Law: Personalized Disclosures in Consumer Law and Privacy Law', University of Chicago Law Review forthcoming, available at SSRN <https://ssrn.com/abstract=3181913>, accessed 17 December 2018; Hermstrüwer, Y (2017), 'Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data', 8 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 9.

[61] For example: Waldman, A (2018), 'Privacy, Notice and Design', Stanford Technology Law Review 1; Hoepman, J (2018), Making Privacy by Design Concrete', in: European Cyber Security Perspectives, available at <http://hdl.handle.net/2066/191716>, accessed 17 December 2018.

[62] For example: Sunstein, C and Thaler, R (2008), Nudge: Improving Decisions About Health, Wealth, and Happiness (Yale University Press); Ménard, J (2010) 'A 'Nudge' for Public Health Ethics: Libertarian Paternalism as a Framework for Ethical Analysis of Public Health Interventions?', Public Health Ethics 3.

[63] Three privacy policies did not have a date, it was therefore not possible to find out when they adjusted their privacy statement for the last time.